Is Cyber Terrorism Coming?[*]

Dorothy E. Denning

May 2, 2002

I will begin my presentation by talking about cyber attacks generally and give you some data about its extent. It is mostly bad news, but I'll talk about just how bad the news is. I will talk a little bit about the reasons for this and the vulnerabilities in computer systems, how cyber protestors are using the Internet in attacks, how terrorists are using the Internet and finally talk about cyber terrorism.

Here is some of the bad news: since 1989, the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie-Mellon University has been compiling data on reported incidents of attacks on the Internet. In the last couple of years, the number of attacks has skyrocketed, approximately doubling in the last year. My understanding is that already in the first quarter of this year, they have received reports of half the number of last year's attacks, so we should see another doubling this year. There were a total of 50,000 last year and each one of those incidents can correspond to an attack that infects thousands or hundreds of thousands computers. Of course, not all incidents are reported to CERT, so that's probably just a small fraction of all attacks.

A firm called Riptech, which provides managed security services, collected data over a six-month period for three hundred clients in twenty-five countries. They looked at different levels of attack, from what are called "informational attacks," which is really people just scanning the Internet looking to see if particular systems are vulnerable but not actually attacking, up to more serious types of attack, including emergencies in which a security breach occurred. Their data showed that almost 40% of the attacks

[*] The views expressed by the author are solely those of the author and may not represent those of any institution with which the author is affiliated.

were targeted at a specific organization or company network. So it's not just kids out there attacking whatever they can; a lot of people are trying to attack very specific places. Riptech's data also show that the intensity of the attacks is increasing, and contrary to some reports, the intensity of attacks did not go down after September 11.

Emergencies, where a security breach had occurred and someone had gotten into the network, were experienced by about 12% of companies. Everybody had the informational kind of attack against them, and almost everybody had warnings, in which an attack bypassed the firewall but did not compromise the system. The majority of the attacks came from persons in the United States, followed by South Korea, China, Germany and France. As for the sources of attacks per capita, Israel was the largest source, followed by Hong Kong, Thailand, South Korea, France and Turkey. China doesn't even show up here.

There is a lot of concern about serious attacks against critical infrastructures. Riptech reported that severe attacks were directed chiefly at the power and energy industries and the financial services industries, both critical infrastructures. The high tech industry follows after that. If you look at attacks from the Middle East, by industry, the power and energy industries are again the most targeted. Financial services are still high, but further down. Since these attacks come from the Middle East, and Israel is a major source of Internet attacks, this could represent attacks from persons in Israel.

The rate of viral infections of e-mails is going up. In 1999, a virus infected one in 1,400 e-mails; in 2001 it is 1 in 300 e-mails. This data comes from an anti-virus company, which scanned their clients' e-mail. They projected that by the year 2015, 3 out of 4 e-mails will have a virus. That is actually very conservative, given the sharp increase that we are seeing. The rate of viral infections of computers is also rising. In 1996, about 10 out of 1,000 computers were infected; last year it was a little over 100 out of 1,000 computers, or about 10%.

It doesn't take a lot of skill to launch viral attacks. You can download free software programs from the Internet that create a virus for you: you run the program, fill in a couple of boxes and you've produced a virus. That's why there are so many viruses – it is that easy. A common type of virus, called a worm, is sent as an attachment to an e-mail; when you open the attachment, it e-mails itself to everybody on your Outlook e-mail address book. There are similarly easy tools for other kinds of attacks. The Code Red worm was one of the costliest viruses, though not the costliest (the costliest was the I Love You virus). The losses caused by the Code Red worm were estimated to be $2.4 billion. It spread quickly across the Internet and ended up infecting 359,000 hosts or computers in a 13-hour period. If you think 13 hours is fast, you can devise a worm with a little more intelligence that will spread in fifteen minutes to an hour. If you get even smarter, you can have a "flash worm" that will hit everything in 30 seconds.

The Code Red worm doesn't spread through e-mail; it just attacks computers, basically mimicking and automating what a hacker would do. If an infected computer is run, it will scan the Internet for vulnerable computers, and when it finds one, it copies itself onto that computer. Once it's on the next computer, it again scans for vulnerable computers and copies itself, and so on. The way a flash worm could spread so much faster is by scanning the entire Internet in advance to identify all the vulnerable computers; the worm would make a list of these machines and as it spreads, it would give part of that list to the next computer down the chain to attack. So there is no wasted effort during the attack phase of scanning for things that aren't vulnerable or that have already been attacked.

Another form of attack is the web defacement. Again, we have seen a dramatic increase in this in the last couple of years. Denial of service (DOS) attacks are increasing as well. The San Diego Supercomputing Center estimated about 4,000 of these DOS attacks take place a week. Most of them last less than an hour but a couple percent of them went on for more than a day.

Why are there so many attacks? As the Internet has grown, there are more people out there to attack and more sites that are potential victims. But it also has a lot to do with the complexity of the systems that are running on these computers. The software has known vulnerabilities and more vulnerabilities are continually being discovered. The attackers are getting increasingly powerful tools and the attacks are easy to perform and have low risk. If you just deface web sites, the chances that anyone will even try to track you down and arrest you are just about nil, because the damages aren't that high most of the time.

One big reason for the increase in the number of attacks is the number of vulnerabilities in the systems. Microsoft, Linux and others all have vulnerabilities. Because Microsoft is used the most, you hear more about it and hackers are more inclined to try to break that system. Vulnerabilities can also appear in the way the system administrators install and operate the software. In addition, user practices create vulnerabilities. Bad passwords are still a major plague on the Internet. A surprising number of people haven't even changed the default passwords they were initially issued, so the hacker knows the default password. Most attacks exploit known vulnerabilities that could be fixed by the operators of the systems. The fixes are available from the vendors, but they haven't been installed.

The number of vulnerabilities reported to CERT has been going up dramatically in the last couple years and has now reached 2,500 over the space of year, which is about seven a day. If you're a network administrator managing a large network for a corporation and you have seven vulnerabilities a day that affect systems across your network, it's a major job to try to handle them, because just patching the patches can cause problems. It's not always straightforward.

A lot of the attacks taking place on the Internet are not carried out by activists or terrorists; they are carried out by kids having fun or by organized criminal groups, which steal credit card

numbers, access banking and financial systems, perform bogus financial transactions, and all kinds of things. Extortion is also happening more and more often, particularly against financial institutions. The attackers get in, get access to credit card numbers or other financial data, and then they threaten to expose the companies or put the sensitive data onto the Internet if the company doesn't pay up. In fact, some do.

Cyber protests have become increasingly common. As conflicts take place in the real world, like those in the Mideast, Kosovo or Kashmir, the spy plane incident with China and so forth, hackers start their own forms of protest, sometimes attacking each other, sometimes, probably more often, attacking government sites in other countries, e-commerce sites or any site they can get access to.

A year ago in October, a Mideast cyber war erupted; it's still going on to some extent, but at a much lower level. In January after the first few months of the cyber war, a local company, iDefense, put out a report listing some of the people who are involved in it, the number of attacks and other data. The pro-Palestinian attackers were primarily targeting commercial sites in Israel and also in the United States. The pro-Israeli attackers were primarily targeting websites that supported terrorist organizations, particularly Hamas and Hezbollah. The pro-Palestinian hackers included Unity and al-Muhajiroun, a London-based group with ties to al-Qaeda.

The Institute for Security Studies at Dartmouth has a major program on cybersecurity and cyber threats. They looked at conflicts taking place in the physical world to see how they correlated with cyber attacks, and they found a pretty good correlation with some of the events.

There is a hacking group based in the UK called the Electrohippies, which has organized several kinds of cyber protest events in the last few years. A few weeks ago, they announced an action against the Israeli government because of Sharon's policies and actions. You can participate in this protest, which is a kind of

denial-of-service attack called a web sit-in. This involves clicking through various sections of their site, which causes your computer to start generating a lot of requests to the targeted Israeli government websites. This produces a lot of traffic against those websites which clogs them up so legitimate traffic can't get to the website. It doesn't really shut down the websites but it slows them down to the point that they're not very useful. This started on April 15 and I think it is still going on.

After September 11, people in cyberspace either tried to express their support for bin Laden or more commonly, people angered by the events of September 11 targeted whatever they could in Afghanistan or neighboring areas. Pro-bin Laden groups, such as the al-Qaeda Alliance Online, appeared. These groups were also involved in the Mideast cyberwar and also in cyberspace skirmishes over Kashmir. G-Force Pakistan, the hacking group that founded al-Qaeda Alliance Online, carried out several web defacements. Their defacements stated that they condemned the events of September 11 but at the same time supported bin Laden and what he stood for. The hackers also listed their demands. Some of their defacements included photos and professional quality graphics.

Various groups also appeared on the anti-terrorist side. One group calling themselves Young Intelligent Hackers Against Terrorism (YIHAT) said they were out to disrupt the money sources for terrorism. They claimed that they had broken into two banks in the Middle East that had accounts for bin Laden. The banks denied it. The YIHAT website asked corporate America to donate their computers to the hackers so that they could use them for cyber attack training, much as al-Qaeda had used the Afghan training camps for terrorist training.

Other anti-terrorist hackers defaced websites supporting the Taliban. Prior to September 11, there were a several sites supporting bin Laden and the Taliban; after September 11, they disappeared as fast as they come up.

Some of the defacements were kind of funny. One of my favorites was a hacker called "Fluffi Bunni", who put the image of a little stuffed bunny on his web defacements. One defacement reads, "If you want to see the Internet again, give us Mr. Bin Laden and $5 million in a brown paper bag. Love, Fluffi B."

A rather large group led by a hacker called "Hacka Jak" from Ohio also targeted websites affiliated with the terrorists. They were one of the first groups out there after September 11 to conduct attacks. The security community pleaded with them not to do this, and there was a press story about this. I was interviewed for it, so my name appeared in the story. So "Hacka Jak" e-mailed me and said we shouldn't be telling him what to do, but lo and behold, this group stopped defacing websites right after that.

Like everybody else, terrorists are using information technology, particularly the Internet. We have seen since September 11 how the hijackers had used e-mail and instant messaging, and had browsed the web to find information about crop dusters and various other things. They also used some information hiding tools so they would be harder to track on the Internet. The Canadian government reported that al-Qaeda was using the Web to search for information about critical infrastructures, in particular management systems like the SCADA system, which provides control on day-to-day acquisitions and things like that. The Aum Shinryko group – they are the ones who carried out a poison gas attack on the Tokyo subway – set up a software development branch and a year or two ago, the Japanese police discovered that this group had written software the police were using. The group was under contract to develop systems for ten government agencies and something like eighty commercial firms.

The Hezbollah website has an English version of their website but a lot of terrorist groups' sites are not in English and you need to able to be able to read the original language they are in. Some of them have areas on their website that are inaccessible to the causal user, because they are password controlled.

Guido Rudolphi, a computer specialist in Switzerland, was researching how al-Qaeda used the Internet and he found a website run by a man named Ould Slahi, who was tied to the Millenium bomb plot against LAX and also to September 11. He was also operating an Internet café. Slahi's website has a guest book that was being used by al-Qaeda operatives to communicate with each other. Rudolphi was tracking activity on that Website and evidently the number of people going to that website and posting messages went up dramatically right before September 11.

I mentioned that many terrorists are using information hiding tools. There have been a few cases reported where encryption has been used to hide communications. The Aum Shinryko cult, again, was pretty good with computers and they had all their files stores stored under encryption.

Government officials have been able to break the encryption in many terrorist cases because the quality of the encryption wasn't very good, basically export grade type encryption. Back around 1996, a lot of the people who opposed export controls on encryption argued that the bad guys wouldn't be dumb enough to use commercial encryption exported from the United States. Folks like me said: "Well, logically that's true, but in practice, it happens." And in fact, it did. I am not trying to argue that we should prohibit exporting encryption programs, but it didn't work out the way people thought it would.

There has been speculation that terrorists are hiding messages in images posted on the Internet. I know one computer scientist who very closely watched a website that supported bin Laden. He examined the images and found that the images looked the same if you looked at them from one day to the next, but if you actually looked at the binary code, the bits that make up those image files, they were changing from day to day. He was never able to crack it but he suspected that there were messages hidden inside the images.

There have been very few cyber attacks committed by people who are known terrorists. There is the case of a terrorist who approached a hacker in 1998 to buy software that had been taken off a Department of Defense computer system, which the hacker claimed could be used to control DOD networks. It was an overstatement of what the software could do but it was nevertheless interesting that somebody tried to buy that program. In another case, IRA hackers broke into British government computers but the purpose there was not to cause destruction but just to collect intelligence and use that in physical attacks. There was an attack against the Sri Lankan embassies' computer systems several years ago. The attackers swamped the embassies with e-mail messages – these are called e-mail bombs. Eight hundred e-mails a day for two weeks was a lot back then. This was more a cyber protest than a terrorist attack.

There were reports of al-Qaeda making cyber threats. A suspected member of al-Qaeda claimed that they had programmers working for Microsoft who had planted Trojan horses in Microsoft code. If in fact they did that, it would have very serious implications: there would be back doors in the Windows program that could then be exploited sometime down the road. It is very unlikely that that occurred, but it's important that it is on their radar screen. It suggests al-Qaeda understands the potential of a cyber attack.

I have left cyber terrorism for the end because I don't think it exists yet, so we are really talking about something that is hypothetical. The Department of Defense defines terrorism as "The calculated use of unlawful violence or the threat of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological." In regard to cyber terrorism, you can translate this two ways. One is to substitute cyber attacks for violence. This waters down the definition; it may not really generate fear and probably won't have the same kind of emotional impact. We can also change the definition by saying that the method will involve some kind of cyber attack. As an example, terrorists might

somehow access the air traffic control systems and alter the flight paths and cause planes to crash. That would have catastrophic consequences in the same way that a physical attack would. Another kind of attack might be something that isn't necessarily catastrophic, but causes major problems on the stock market or affects the financial community in some way so as to generate a similar level of fear.

The best work on cyber terrorism has been done by the Center for the Study of Terrorism and Irregular Warfare (CSTIW) at the Naval Postgraduate School. They produced a report in 1999 that assessed the prospects of terrorist groups pursuing cyber methods. They concluded that the barrier for entry was actually fairly high, aside from the kind of skirmishes that we see the hackers doing now. Terrorists generally lack the wherewithal, including human capital. The NPS study looked at different levels of cyber terror capability, from very simple hacks, like you see taking place now, which don't really require any skill at all, up to more sophisticated kinds of attacks that might take several years to develop.

They concluded that religious groups were the most likely to seek the most advanced capabilities, consistent with the indiscriminate use of violence. Ethno-nationalist, separatist and revolutionary groups are also likely to seek advanced, structured capabilities. So far the New Age groups like the animal rights activists are just engaging in cyber protests and disruption.

In May 2000, the CSTIW held a conference to assess whether or not sub-state groups engaged in armed resistance would pursue cyber terrorism. They invited some practitioners from those groups to participate in the workshop: two from the Basque separatist movement, one each from the PLO, the Tamil Tigers, and the Columbian revolutionary group FARC, one hacker, eleven academics and one UN representative.

They originally scheduled a second conference the week of September 11 to look at religious groups. I had been invited to

participate but I couldn't because of a conflict. After September 11, I learned they had cancelled it earlier.

In the meeting they held the year before, they developed a simulation based on the situation in Chechnya. In that simulation, the group representing the Chechen resistance had advocated doing only one kind of cyber attack, namely some kind of disruption that would affect the Russian stock market. They decided not to do more than that was because they didn't want to do something that would impact the average Russian, whereas an attack on the Russian stock exchange would only affect the elite. The conclusions from that study were consistent with the conclusions from their earlier work.

My conclusions are very similar: the Internet is very vulnerable to serious attack. There is no question about it. Whether it will be terrorists who attack it, I am not so sure, but I think we will continue to see a lot of hacking and attacks by organized crime where there is the possibility of a big payoff. Down the road, there is potential for terrorists engaging more in cyber attacks. A lot of the attacks that have been postulated would be a lot more difficult to pull off than you might be led to believe from reading reports in the press.

One of the most serious incidents took place in Australia a year or two ago, where a man was able to hack into the sewage control system and reverse the flows of sewage, which harmed the environment and killed wildlife. He didn't have any social or political agenda; he was mad because he had been turned down for a job with the county that operated the sewage system. This was his revenge. He was able to pull this off because he had worked for the company that wrote the software and had taken it home when he left the company. He had knowledge and tools that not anybody could have obtained. Furthermore, it took him forty-six tries to get it. This is good news in a way: interfering with the system wasn't that easy even for somebody who had the software and knew what to do. It gives an indication, I think, that a serious attack can't be done just by anybody; it really requires some inside

knowledge. On the other hand, insiders can be bought. We have had plenty of spies in this country who have sold information to foreign governments. We can't assume that people who are working in the areas of critical infrastructures might not turn on them in some way that would lead to a major attack.

# # #

Question & Answer Period

Question: How effective are off the shelf security systems, like the Norton anti-virus program?

Denning: I think most of the major products are very good. I use Norton myself. You do have to keep them up to date because viruses are continually evolving, not by themselves, but because attackers write new viruses that the anti-virus program won't detect. My approach has been not to use Outlook for my e-mail. I don't use Internet Explorer; I use Netscape. I don't know if that has made me less vulnerable or not. My husband uses a Macintosh, and that will also prevent a lot of attacks.

Question: Are the critical industries, the financial services and energy and power, investing enough to significantly reduce their vulnerabilities?

Denning: I can't answer whether they are investing enough. I know they certainly pay more attention to it now than they have in the past and there's definitely increased awareness of it.

Question: You mentioned the issue of state-sponsored terrorism. I agree with your points about the difficulty for individual people to accomplish much beyond the ankle biting, nuisance kind of attack. On the other hand, state-sponsored hackers would be bringing a lot more resources to bear, particularly in compromising insiders, and the insider threat is really the key one. If we thought that security

classification systems and getting security clearances was tough before, there's a whole new dimension of clearance and background checks that are going to need to be done for a new class of people. But there are countries that are able to do this. I would think it would be in their interest to penetrate but not necessarily do anything, just so they know where to go when they decide they want to, at the right time. Do you have any general thoughts about state-sponsored terrorism?

Denning: We certainly know that some of the major states are looking at cyber methods. Certainly China is one; Russia is another one. I have heard that Iraq is looking at these things.

Question: And maybe the United States.

Denning: The United States has been looking at it for years, absolutely. None of this is surprising; any country that is not looking at it would be asleep at the wheel. You have to understand and study the attacks if you want to defend against them. And you might want to launch an attack. In terms of state-sponsored terrorism, I don't worry about China on that. They have good reasons not to want to interfere with the West's infrastructure, which would have global impact. If you disrupt the stock exchange in the United States, it will affect stocks worldwide. If you shut down electricity across the United States, the stock market is going to go down, business will come to a halt, and that will have global implications. So to me, any country would be crazy to do something that would have a major impact on infrastructure. But that doesn't mean that a terrorist group, or a country that feels like it has nothing to lose globally by causing that kind of major disruption, won't.

Question: If you connected to an Internet provider through a modem, they can't attack you, unless you're actually connected, isn't that right?

Denning; You have to be connected in order to be attacked, that's true.

Question: Most ordinary computer users don't know anything about firewalls and don't have them. And if they have an anti-virus program, they probably don't keep it up to date. There's a lot of vulnerability out there. Couldn't Microsoft and the other companies put something in that would help in this regard? That ought to be part of the operating system in some way, or at least a system to alert you if you're being attacked.

Denning: Many of the attacks are hitting at the application layer there, so you can't put it all in the operating system. Microsoft is in a bad position because the more they do, the more people say they are taking over the market. There is a good business now in the anti-viral business by itself.

Somebody suggested that it should be illegal to operate a computer without keeping your anti-viral tools up to date. If your computer spreads a virus and your anti-viral tools weren't up to date, you could be perhaps fined or found guilty of a misdemeanor. I don't like that idea, mainly because I don't always update mine every two weeks. If I do good hygiene on my computer, nobody is going to infect it; I can defend myself against other people's viruses. Should you need a license, like a driver's license, to operate a computer on the Internet? In this case, you would need to renew it, not once every three years or five years, but every two weeks or month to show that your computer is safe.

Question: One of the initiatives that's been kicked around lately is to have the government take a more active role with industry to alert people and get them to report attacks to the government, to try to get a coordinated alert system. Do you think that would be effective?

Denning: I think it is a great idea. The FBI now says they have over 4,000 members in their InfraGard program, which is set up with all the field offices. Industry itself has set up Information Sharing and Analysis Centers (ISACs) for reporting within the industry and these all seem like great steps forward to address the problems. But you need anonymity in the reporting or companies won't report. The FBI says that people can make anonymous re-

ports and then that information can be shared with other members anonymously. The FBI also says that they can protect corporate information from the Freedom of Information Act. A lot of corporations aren't convinced of that and so there has been some effort made to get that explicitly stated in law. The FBI says that they can do it.

Question: I agree with your assessment that terrorists are less likely to use cyber terrorism as a tool. Two years ago the Denial-of-Service attacks on Yahoo and the e-commerce sites were described as "cyber terrorism." That was a cruel, malicious event, but we need a better term than cyber terrorism. I don't know what the word is.

Denning: I would call this kind of attack "cyber vandalism."

Question: We had a discussion at the National Defense University right after 9/11 and we concluded that they could have taken down the communication infrastructure by interfering with the FAA system. The FAA system is secure for patrolling aircraft, but if you take down the communication structure that the FAA system depends on, you could make people afraid of secondary and tertiary attacks, because they would not know if all the aircraft were brought down. The Pentagon was evacuated three additional times because we didn't know if something else was coming in. They missed the opportunity to make their attack even worse by simultaneously launching this kind of attack.

Denning: But that would have been much, much harder.

Question: They did a great deal of planning for that single event. Considering the amount of time they had in planning that one event, they missed the opportunity. I really don't think they understood that. We may be helping to educate them with this kind of discussion.

Denning: I don't know how they would get the education to do that. You can see how they got the education to fly the airplanes;

anybody can do that. But where would you get the knowledge to take down the FAA's communication system?

Question: Look at the areas they might target, such as, computer science. How many students in this field are US citizens? Are we training the next wave of terrorists in our universities? They won't be using hacker tools available over the website. They are actually studying the systems, identifying vulnerabilities. The "Code Red" virus was very disruptive but there was no payload associated with it. If it had a destructive payload, it could have taken down the Net. "Code Red #2" was another test firing of a missile, but still had no payload. The next missile may have a payload.

Denning: Yes, it could, but it wouldn't have had as much impact, because it would have knocked itself out. "Code Red" spreads by attacking other computers; if it kills off its host, it can't do that. It might carry out five attacks and then kill off the host, but then it's not going to spread as fast. People have postulated a lot of smarter ways of carrying out attacks: you could infect the hosts with a virus that includes a time bomb which is hidden in the system someplace and goes off on a specific day.

Question: Do you have any ideas about what sort of research needs to be done or what actions need to be done to protect against future cyber terror attacks?

Denning: That is almost unlimited. We always need new and better defenses methods because the hackers are creating new and better attacks. One of the things that we need is empirical data to define good security practices. Right now, security is pretty ad hoc. A lot of the reason why corporations haven't been quick to tighten security on their networks is there hasn't been an economic case made to do it. Nobody has shown that if you follow a specific plan of action, you will get a specific return on your investment and protection against loss. It's difficult for a company to know how much money to spend, which products to buy, and how much they will save by doing that. A lot of work has to be done to establish

empirically grounded best practices and what we need to do to protect our networks.