Cyber terrorism — fact or fiction?

Cyber terrorism is no longer the stuff of science fiction in this age of information technology. All a hacker needs is a motive and the impetus to exploit the susceptibilities of computer networks to cause mass disruption

BY SOOBIA AFROZ

DT. Dawn 16.6.02

A FEW well-planned keystrokes at the keyboard, some source code glued together from different virus variants, a little know-how about networking and lo and behold! — out comes the newest form of terrorism of the digital era, cyber terrorism.

A term coined by computer whiz Barry C. Collin, cyber terrorism is no longer the stuff of science fiction. The threat is present and very real, especially because of the phenomenal growth of the Internet that has given millions of people access to computer networks. Experts say that within a short span of ten to twenty years, we may look back at the present generation of terrorists and think that their methods of terrorism were rudimentary.

The modern terrorist is not only seeking weapons of mass mayhem he can cause is unlimited. The number of hackers who break into various government and private industry computer networks and key communications systems on a daily basis demonstrates the weaknesses in these systems.

Information has become the ultimate weapon in today's

include hack threats, mail bombs, spam, harassment, forgery, virus, denial of service, destruction and intrusions. By cracking into a government or military websites, hacktivists can now use cyberspace to threaten various governments.

can do just that. If a cyber terrorist hacks into a computer system that controls a city's power supply, or telecommunications network, or aviation system, or financial network, then the

of their organization's to make a point. Usually, their targets are government websites, which they vandalize to protest against the government's policies. Other forms of computer abuses

steal important information by taking advantage of weaknesses in the infrastructure.

Computer viruses are a common menace on the Internet, and a very attractive tool for cyber-terrorists. In 1999, a virus named 'Melissa' infected about a million computers and

clogged networks in the United States, causing $80 million in damages. Then, in May 2000, a more lethal virus, the infamous 'Love Bug' spread like the literal wild fire across tens of thousands of computers over the Internet. The virus originated in an email titled 'I love you' and

ists and think that their methods of terrorism were rudimentary. Fast forward a decade, and the ultimate weapon of power and influence will be information. In the wrong hands, information will prove destructive for not only individuals, but for governments as well.

Information warfare will become the fundamental form of combat in the near future, especially as more and more governments are becoming technology-dependent. With the increasing computerization of major government systems and the vast body of data available on the Internet, it will only take a hacker to put together the motive, the mode and the impetus to exploit the susceptibilities of computer networks to cause disruption. It is not only the individual hackers or terrorists who might take up this form of terrorism, foreign governments might also use this tool to destabilize rivals. According to a BBC report, in countries like China, some military strategists have called for the use of 'unconventional measures' to counterbalance the military prowess of the United States.

Cyber terrorism is just like any other crime, only it affects people strategically, not physically. Terrorism means causing widespread havoc among people, and cyber terrorism

The modern terrorist is not only seeking weapons of mass destruction, but 'mass disruption' as well. Blowing up buildings and taking up hostages may soon become a thing of the past as the definition of terrorism moves into the information arena. What makes this form of terrorism so attractive to today's terrorist is the fact that it is much easier to stage than conventional terrorism.

A computer-based attack can take place while the perpetrator is many thousands of miles away from his target, and the Internet offers a very convenient tool to bridge this distance. This creates a major challenge for law enforcement agencies, because attacks of this nature cannot be tracked via the classical intelligence methods. To trace such an attack back to its originator would require following the original command back through the computer network or the Internet. But, many Internet service providers don't keep any log data, so the data on an Internet user's activities is not easily available, thereby erasing any electronic trail leading to the perpetrator.

A common form of cyber terrorism is called 'hacktivism', where terrorist organizations break into important websites, deface them and replace the content with that

Information has become the ultimate weapon in today's world of digital revolution. The World Wide Web is a vast repository of statistics, facts and figures, therefore, information about anything and everything is just a click away. In the wrong hands, this information can prove lethal. After the September 11 fiasco, the US government has removed sensitive documents and reports from websites across the Internet, due to the concerns that the data may prove useful to terrorists planning further attacks. Information about hazardous chemicals, maps, location and layout of military bases, chemical weapons facilities and intelligence offices has been pulled out of the web, by not only the various US Government sites, but private US websites as well. Other data that has been removed includes information that could help terrorists identify targets and plan attacks.

The problem that hundreds of networks connected to the Net face everyday is that they are under attack by automatic software tools looking for and exploiting the vulnerabilities they find. Such virus outbreaks are threatening to overwhelm web-based servers. Attackers are acquiring more sophisticated tools to crash networks by flooding them with bogus traffic and

contained an attachment, which, when opened, sent copies of the same email to everybody listed in the user's address book. Some viruses are designed to delete the entire hard drives, but the 'Love Bug' was not designed to do that. Instead, it caused damage because of the way and with the speed it propagated, consequently clogging the e-mail systems. Many large corporations had to shut down their email systems to safeguard against the virus.

Large corporations and multi-national firms are also at risk from cyber terrorists. The world's most powerful technology company, Microsoft, has been a particular target. Unknown hackers gained access to the source code to Microsoft's valuable software, including the latest versions of Windows and MS Office. While the hackers were able to see the source code, they could not make any changes in it. However, this break-in is a major sign that even the world's software giant is not safe from cyber-attacks. The consequences of this sort of attack on Microsoft are far-reaching. Gaining access to Microsoft's source code could, in theory, enable the hackers to construct their own software, or sell the code to Microsoft's competitors. The hackers could also stage a 'data hostage" ploy, in which, they would try to blackmail Microsoft into paying to get back any stolen codes.

Cyber vandals are imaginative and resourceful in their methods. One such method is the usage of automatic tools that sweep the Net, via instant messaging software such as IRC, on behalf of the attackers. Mobile phones and personal digital assistants (PDAs) may be their next targets. Security analysts warn that viruses, even the one like the Love Bug, are too complex to run on today's mobile phones. Hackers may want to use cell phones and personal digital assistants to break into networks, as cell-phone technology evolves into wireless application protocol (WAP), which now comes with extended memory, increased power and connectivity. A small glimpse of this capability was displayed in 2000, when Nokia handsets froze after receiving a certain text message. Mobile phones are especially vulnerable to attacks because they are always online and because they are popular with a large number of users. In future, the combined mobile device of a phone and PDA may become powerful enough to be used as a gateway to the corporate network to run viruses.

Even though no major human tragedy has been caused by cyber terrorism to date, the pace at which technology is evolving is a sign of what the future may hold for information warfare. There are sceptics too, who reject the possibility of an 'Electronic Pearl Harbour', a term used to describe an extremely lethal and deadly cyber-attack. They argue that over the years, computer systems have become more secure and reliable. They dismiss the cyber terrorism threat as exaggerated and unrealistic. But, no matter what they say, most of the governments are taking cyber-warfare seriously, and adopting a 'prevention-is-better-than-cure' strategy by employing more rigorous security measures to safeguard important computer systems. As the world becomes interconnected and more reliant on the computer networks, we will need to be more careful in terms of reliability and security. Because there will always be someone out there wanting to take advantage of some weakness or loophole in the system, or a unique way to break into a network. ■