SPECIAL REPORT

Health Implications of Cyber-Terrorism

A. Clem, MPH, MSN;[1] Sagar Galwankar, DNB (India), MPH;[2] George Buck, PhD[3]

1. Department of Environmental and Occupational Health, College of Public Health, University of South Florida, Tampa, Florida USA
2. Assistant Professor of Medicine, Division of Infectious Diseases, Department of Internal Medicine, College of Medicine, University of South Florida, Tampa, Florida USA
3. Associate Professor of Environmental and Occupational Health, College of Public Health, University of South Florida, Tampa, Florida

Correspondence:
Sagar Galwankar, DNB (India), MPH
193, Mountain View Drive,
Clifton, NJ 07013 USA
E-mail: sgalwank@hsc.usf.edu

Keywords: cyber-terrorism; health; healthcare; terrorism

Abbreviations:
DoS = denial of service
EMS = Emergency Medical Services
HIPAA = [US]Health Insurance Portability and Accountability Act
OAM&P = operations, administration, maintenance, and provisioning
SCADA = supervisory control and data acquisition
US = United States of America

Web publication: 15 March 2004

Abstract

The world is becoming ever more interconnected via the Internet, creating both benefits and disadvantages for human communities. This article examines cyber-terrorism, one of the major negative consequences of the Internet. It also examines the potential impact of cyber-terrorism on the health of populations, its possible perpetrators, and its prevention and control.

Clem A, Galwankar S, Buck G: Health implications of cyber-terrorism. *Prehosp Disast Med* **2003;18(3):272–275.**

Introduction

The Internet has brought revolutionary changes to the world. One of the greatest changes has been the growing connectivity between all "corners" of the world via the Internet. In many ways, this has been a boon to humanity. The Internet has allowed the expansion of communication and the transfer of knowledge throughout the world at a rate never before achieved. However, there also has been a dark side to this achievement. A prime example of this negative side has been the rapid spread of computer viruses, such as the Melissa Macro Virus, the Bugbear virus, and the MSBlaster worm. As the world becomes more dependent on the myriad activities carried out via the Internet, the potential exists for much more serious consequences of this "dark side" of the Internet, including events related to cyber-terrorism.

In response to this perceived cyber-threat, governments, industries, and other institutions have implemented a variety of security measures. Meanwhile, criminal hackers, or "crackers", have become ever more inventive at circumventing these security systems. Today, most contemporary terrorism-related events occur in the physical world via physical weapons, such as explosives or chemical agents. In the near future, it may be possible to harness the connectivity of the Internet to disable certain key computer systems and cause similar amounts of damage at much less risk to the attacker. For example, if a group wanted to disable an emergency medical services (EMS) dispatch center, would it be easier and less risky for the attacker to destroy it with explosives or to disable its computer systems with a computer virus?

This article examines cyber-terrorism, one of the major negative consequences of the Internet. It also examines the potential impact of cyber-terrorism on the health of populations, its possible perpetrators, and its prevention and control.

What is Cyber-terrorism?

A spectrum of criminal acts may be conducted via the Internet, ranging from cyber-espionage and information warfare carried out by foreign governments to cyber-crimes carried out by smaller groups or individuals. Although cyber-terrorism may be carried in conjunction with cyber-espionage or cyber-crime, it is considered distinct from the two entities. Cyber-terrorism combines both

cyber-space and terrorism and may be defined as the use of intentional violence against computer systems that support or protect the health of human communities or the information stored in these systems. Unlike cyber-espionage, virtually all instances of cyber-terrorism to date have been carried out by organized factions unconnected to world governments. Often, cyber-terrorism is aimed at coercing a population or its government to accede to certain political or social objectives. In addition, cyber-terrorism usually is more extensive and destructive than is simple cyber-crime.[1] As a result, cyber-terrorism either harms the health of human communities or generates a fear of this harm.[2]

Cyber-terrorism still is in its infancy. Although there have been numerous cyber-terrorist events, there have been no large-scale incidents affecting large geographic areas. Despite the challenge of producing damage of this magnitude, the potential for a large-scale, cyber-terrorist event increases as the Internet continues to expand. Furthermore, cyber-terrorism may be used to: (1) help plan other terrorist activities; (2) soften a target prior to a physical attack; or (3) generate more fear and confusion concurrent with other terrorist acts.[3]

To date, relatively few terrorist attacks have taken place against the healthcare infrastructure of countries — even in geographic areas or countries with a high burden of terrorist attacks. Despite several notable exceptions in recent years, including direct attacks on first responders via secondary explosive devices and bombings of hospitals and health clinics, most terrorist groups have avoided attacking the most vulnerable civilian populations, such as hospitals, schools, and elder-care facilities. On the other hand, cyber-terrorism has the potential to enable terrorists to attack healthcare facilities with much greater ease and with less moral outrage than would occur with actual physical attacks.

Until now, incursions into medical records have been considered as cyber-crimes rather than cyber-terrorism. However, with the increasing use of the Internet for telemedicine and the storage of medical and health insurance records in computer systems, the possibility of attacks on these records becomes more likely. As a result, cyber-terrorism has the potential to alter or destroy individual medical or health insurance records, alter computer-based prescriptions at pharmacies to life-threatening doses, or make private medical records public that otherwise would remain confidential under current Health Insurance Portability and Accountability Act (HIPAA) regulations.

Potential Cyber-terrorists

Cyber-terrorism potentially can be carried out by anyone with access to the Internet. This includes anyone with a computer (and a modem), and as the technology becomes more sophisticated, may include anyone with cellular phones, wireless personal digital assistant (PDAs), and other wireless, handheld devices. The next cyber-terrorist may be a world away or right nextdoor as long as they have Internet access and the requisite knowledge. Accordingly, cyber-terrorists may be domestic or foreign, with few limits on their actual location.[1]

Cyber-terrorists may act alone, as members of terrorist groups, or as proxies for terrorist groups.[1] For example, in Hanover, Germany in the 1980s, crackers hired out their services to a terrorist group.[1] Potential cyber-terrorists also may include disgruntled current or former employees of a variety of private or public institutions.

Cyber-terrorists are likely to be very comfortable with using computers and the Internet. In everyday life, people use the tools that they know and are comfortable with, including tools for criminal or destructive activities. As the Internet becomes an increasingly more central part of daily life, future terrorists increasingly will be more likely to use the Internet to plan and carry out terrorist activities. Why endanger one's life with explosives or weapons of mass destruction when you can sit in front of a computer and attack your enemy with almost total anonymity?

Today, most criminal hacking, or "cracking", is accomplished by one of three methods: (1) DoS (denial of service) in which the attacker overloads the server and shuts the system down; (2) actual destruction of information (although erasure of information usually is difficult to do effectively if their back-up systems are in place); and (3) alteration of information, or "spoofing", (which is more difficult to safeguard against, but also can be mitigated with the use of backup systems).[5]

Hackers are able to access computers via a number of routes, including poorly protected passwords, liberal access privileges, or dormant accounts of former employees.[6] Hacking is facilitated by laxly enforced security policies. Currently, "parasites" are of great concern as a type of cyber attack. Parasites are small computer programs that remain in computer systems and slowly corrupt the system and its backups, thus, damaging the information in the system. These parasitic programs can cause systems to perform the wrong tasks. They also can spoof data, thus causing record alterations with untoward effects.[3]

Much of the basic knowledge needed to carry out acts of cyber-terrorism is readily available through the Internet. Many hacking tools can be downloaded freely from the Internet through quick and easy searches. According to Jane's Intelligence Review, the absolute beginner requires only knowledge of English and the capability to follow directions.[5] However, in order to crack the better-protected computer systems ("hardened systems"), more extensive knowledge is required. This includes several years of experience with computer languages (e.g., C, C++, Perl, and Java), an understanding of general UNIX and NT systems administration, local-area network/wide-area network theory, remote access and common security protocols, and sufficient time would be required. Much of this advanced education and training also is available over the Internet or may be obtained through readily available classes at public educational facilities.

Potential Effects

Cyber-terrorism has the potential to greatly affect the healthcare infrastructure of a modern society. In many countries, as healthcare systems have become rapidly more dependent on

the Internet, a number of instances of cyber-crimes against healthcare systems already have been reported.[2] While to date, most cyber-crimes have been minor, they likely are harbingers of acts to come. Areas of particular concern to healthcare facilities include the potential for cyber-terrorism-related events to erase or alter computerized medical, pharmacy, or health insurance records.

Cyber-terrorism also may target other institutions that directly or indirectly affect the health of communities. Industries or public service agencies at particular risk of cyber-terrorism include: (1) water supply; (2) electrical power supply; (3) emergency services; (4) telecommunications systems; (5) transportation systems; (6) banking and financial systems; and (7) government.[7]

The potential for cyber-terrorism to cause widespread mayhem with public health and safety implications is illustrated aptly in the following passage:

> There have been numerous attacks against these infrastructures. Hackers have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration, maintenance, and provisioning (OAM&P). They have crashed or disrupted signal transfer points, traffic switches, OAM&P systems, and other network elements. They have planted "time bomb" programs designed to shut down major switching hubs, disrupted emergency 911 services throughout the eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan. They have installed wiretaps, rerouted phone calls, changed the greetings on voice mail systems, taken over voice mailboxes, and made free long-distance calls at their victims' expense – sticking some victims with phone bills in the hundreds of thousands of dollars. When they can't crack the technology, they use 'social engineering' to con employees into giving them access.[2]

Cyber-terrorism against the telecommunications system may have critical implications for the public health of communities. From the healthcare system perspective, attacks against the telecommunications system not only have the potential to disrupt the flow of health information, but also the multiple logistical systems upon which the operations of healthcare facilities depend (e.g., the acquisition of supplies). From the public safety perspective, cyber attacks against the telecommunications system may disrupt crucial information-sharing networks. For example, in March 1997, a teenage hacker penetrated and disabled a telephone company computer that provided service to the Worcester Airport in Massachusetts, cutting off service to the airport control tower, fire department, security, and weather service for six hours.[2]

Public safety may be affected adversely by cyber-terrorism in other ways. For example, in 1992, a disgruntled former employee of Chevron Corporation's emergency alert network, hacked into computers in New York and San Jose, California and reconfigured the firm's emergency alert system so that it would fail during an event.[2] The disabled system was not discovered until an emergency arose at the Chevron refinery in Richmond, California and the adjacent community could not be notified during an accidental chemical release. During the ten-hour period in which the system was down, thousands of people in 22 states and six areas in Canada with Chevron facilities went without the Chevron emergency alert system. As suggested above, hackers also have attacked traffic regulation systems, disrupting traffic lights, with the potential for an increase in motor vehicle collisions.

Cyber attacks against the essential services, such as the water and electrical supply systems, comprise another major area of concern. Hospitals and communities alike are highly dependent on water and only can subsist for limited periods without water. Fortunately, the majority of water system authorities in the United States of America (US) are protected against cyber attacks by supervisory control and data acquisition (SCADA) systems, through these systems still may be circumvented by other means.[3] While hospitals in the US almost always have back-up generators should the electrical supply system fail, communities almost always are immediately vulnerable. The longer a community remains without power, the more likely it is to suffer food and selected medication spoilage due to loss of refrigeration and deaths due to medical equipment failure (i.e., ventilators outside of hospitals).

Finally, cyber-terrorism also can cause environmental contamination, with the potential for adverse health effects in the community. For example, in 2000, a perpetrator in Australia allegedly penetrated the Maroochy Shire Council's computer system and used radio transmissions to create overflows of raw sewage into the Sunshine Coast, causing widespread contamination.[2] By extrapolation, a dedicated terrorist group could use cyberterrorism to cause more widespread, more enduring, or more toxic environmental contamination, with an almost incalculable impact on public health.

Prevention and Control

Up-to-date computer security systems and firewalls, personal vigilance, and adherence to best-practice guidelines are essential in maintaining the security of computer systems.[8] While the knowledge of how to hack into a computer system is readily available on the Internet, this same knowledge also allows systems managers to understand how better to protect their systems. In addition, the Internet offers many resources, which can assist in protecting computer systems from cyber attacks. Nevertheless, even with the best security systems, safety measures can be rendered ineffective by lapses in security-conscious behavior.

Conclusion

At the present time, the actual health implications of cyber-terrorism only can be conjectured. Nevertheless, terrorism has evolved rapidly in recent years parallel with the expansion of human knowledge. Facilitated by the Internet, this expansion of knowledge has had numerous benefits for the health of human communities. However, as terrorists realize the untapped potential of the Internet, the burden of cyber-terrorism is likely to grow. Based on current trends, in the future, it is likely that cyber-terrorism events will occur that have not yet even been contemplated. To be forewarned is to be prepared.

References

1. Rattray G J: Chapter 5. The cyber-terrorism threat. Available at www.securityunit.com/asale/inss/terrchp5.html. Accessed 25 June 2003.
2. Denning DE: Cyber-terrorism (2000). Available at www.cs.georgetown.edu/~denning/infosec/cyberterror.html. Accessed 25 June 2003.
3. Berinato S: The truth about cyber-terrorism (2002). Available at www.cio.com/archive/031502/truth.html. Accessed 25 June 2003.
4. Anonymous: The basics of terrorism. Available at www.isuisse.ifrance.com/emmaf/base/baster.html. Accessed 25 June 2003.
5. Jane's Intelligence Review: Cyber-terrorism hype (1999). Available at www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm. Accessed 25 June 2003.
6. Cunningham K. Cyber-terrorism: Are we leaving the keys out? (2002). Available at www.scmagazine.com/scmagazine/sc-online/2002/article/51/article.htm. Accessed 25 June 2003.
7. Lawson SM. Information warfare: An analysis of the threat of cyber-terrorism towards the US critical infrastructure (2002). Available at www.sans.org/rr/papers/29/821.pdf. Accessed 25 June 2003.
8. Vaughn-Perling J. Network security: A new virtual foot solider against cyber-terrorism. Available at www.infosecnews.com/opinion/2002 /04/03_04.htm. Accessed 24 June 2003.