Stopping Cyberterror

COUNTRIES MUST WORK TOGETHER TO THWART EFFORTS OF INTERNET CRIMINALS

Dr. Viacheslav Dziundziuk, professor, Kharkhiv Regional Institute of the National Academy of Public Administration (Ukraine)

PER CONCORDIAM ILLUSTRATION

Cybercrime encompasses crimes in the so-called "virtual space." Virtual space (or cyberspace) may be defined as a computer-modeled information space containing information about individuals, subjects, facts, events, phenomena and processes presented in a mathematical, symbolic or any other form and circulating in local or global computer networks, or data contained in the memory of any physical or virtual device or any other medium specifically designed to store, process and transmit those data.[1]

In contrast to traditional types of crimes whose history goes back many centuries, such as murder or theft, cybercrime is a relatively recent phenomenon that appeared with the creation of the Internet. It bears mentioning that the very nature of the Internet is conducive to committing crimes. Its global reach, ability to transcend borders and reach a broad audience, anonymity of its users, and distribution of major network nodes and interchangeability create advantages for criminals and allow them to hide effectively from law enforcement agencies.

The first computer criminals, later called "hackers," appeared in the 1970s. It's difficult to say exactly who the first hacker was, but most sources cite John Draper as the first professional hacker. He also created the first hacker specialty — "phreakers," from "phone hacker." Among the ranks of the hackers of the time were such well-known figures as Steve Wozniak and Steve Jobs, who would later go on to found Apple Inc. *Phreakers set up the production of devices to intrude into home telephone networks. This period can be considered the beginning of the development of computer crime.*

The first widely publicized arrest of an Internet criminal occurred in 1983 in the city of Milwaukee in the United States. The case was the first recorded Internet hack, committed by six teenagers who called themselves the "414 Group" (414 was the Milwaukee area code). Over nine days they hacked into 60 computers, some of which belonged to Los Alamos National Laboratory. After the arrest, one group member testified against the others, who received suspended sentences.[2]

The very nature of the Internet is conducive to committing crimes.

In the 1980s, we began to see a major increase in computer attacks. For example, although Internet users made only six complaints of computer attacks to the CERT Internet security center in 1988 (the year the center opened), there were 132 complaints in 1989, and 252 in 1990. Cybercrime was no longer a rarity. Large hacker groups were coming on the scene, and the Internet began to be used to commit a wider range of crimes. *This was the beginning of the second phase of the development of cybercrime, characterized by new areas of specialization for Internet criminals.*

In 1984, Fred Cohen published information about the development of the first malicious self-replicating computer programs and used the term "computer virus" to describe them. He also wrote a program that demonstrated the possibility of one computer infecting another.

In 1986, a member of the group "Legion of Doom," Loyd Blankenship, known as "Mentor," was arrested. During his incarceration, he wrote the famous "The Hacker Manifesto."[3] The ideas espoused in this manifesto are considered to this day to underlie the hacker ideology and culture and are widely distributed throughout the Internet. Clearly, a quantitative rise in cybercrimes coincided with the increased popularity of hacker ideas in the computer world, which attests to the interconnection between these phenomena.

In 1994, the world learned of the Vladimir Levin case, categorized by investigators as a "transnational computer network crime." An international criminal group of 12 people using the Internet and the Sprint/Telenet data transmission network breached a protection system and attempted to make 40 transfers totaling $10.7 million from the accounts of bank clients in nine countries to accounts in the United States, Finland, Israel, Switzerland, Germany, Russia and the Netherlands.[4] This was the first major international financial crime using the Internet to become known to the general public. It demonstrated that cybercrimes can cause serious financial damage. In 1998, a 12-year-old hacker penetrated the computer system controlling the floodgates of the Theodore Roosevelt Dam in Arizona. Opening the dam's water-release gates could have inundated the U.S. cities of Tempe and Mesa, Arizona, which had a population of more than 1 million.[5] This incident gave rise to such terms as "Internet terrorism," "computer terrorism" and "cyberterrorism." It also demonstrated that the Internet itself is most vulnerable to cyber attacks, as its key components are accessible from anywhere in the world. This fact does not escape the attention of hackers.

The Internet itself is most vulnerable to cyber attacks, as its key components are accessible from anywhere in the world. This fact does not escape the attention of hackers.

THE INTERNATIONAL THREAT

The emergence of cyberterrorism and highly publicized cases of crime by international groups provide evidence that cybercrime is now transnational. This represents the beginning of the third phase in the evolution of cybercrime.

It is alarming that with the development of the Internet, serious consequences can ensue, not only from intentional cyber attacks but also from the carelessness of professionals. For example, in 1997, a mistake by an employee of Network Solutions resulted in sites with names ending in .net and .com becoming inaccessible. That is, the operation of the entire World Wide Web was disrupted owing to the carelessness of a single individual.

At the same time, cyber attacks are becoming a means to achieving political ends. A typical example is Internet stoppage in which perpetrators simultaneously log onto a site, connect to a server, send an e-mail or make postings to forums in order to limit or even deny access to the site by other users. The Internet site or server is overwhelmed by access requests, causing an interruption or complete stoppage.

The first such attack was carried out by a group calling itself the "Strano Network," protesting against the French government's nuclear and social policies. In the course of one hour, on December 21, 1995, the group attacked the sites of various government agencies. Group members from around the world were instructed to use their browsers to visit government sites simultaneously. As a result, some sites were indeed shut down for a time.[6]

The transnational aspects of cybercrime continue to manifest themselves more widely. The conflict in Kosovo can be considered the first Internet war, in which various groups of computer activists used the Internet to condemn actions of both Yugoslavia and NATO, and in doing so, intentionally impeded the operation of government computers and gained control over sites. This was followed by a "deface," a change in the site's content. At the same time, stories about the dangers and horrors of the war, as well as facts and opinions of political leaders and public figures, circulated through the Internet. This served as propaganda to a wide audience throughout the world.[7] All this is characteristic of the third phase of the development of cybercrime.

It should be noted that today practically any military or political conflict is accompanied by organized opposition on the Internet. For example, in 2005, there was a wave of cyber attacks prompted by a school history textbook issued in Japan that presented a distorted account of events in China from 1930 to 1940 by ignoring war crimes committed by Japanese forces during the occupation. Among the targets of the attacks were Japanese ministries and agencies, sites belonging to large Japanese corporations, and sites devoted to World War II. In this case, the Chinese hackers displayed a high degree of organization, as evidenced by the synchronicity and massive nature of their attacks. Considering that the state controls the Internet in China, this attack was presumably sanctioned by the government. *The use of cyber attacks for political ends may be considered the beginning of a fourth phase in the development of cybercrime.*

The China example was copied by Russian hackers who carried out several large-scale distributed denial of service attacks. Estonian government sites were attacked over a period of a few days in late April and early May of 2007. A youth movement called "Nashi"[8] claimed responsibility. And in August 2009, the U.S. publication *Aviation Week* accused Russian hackers of attacking the server for the Baku-Tbilisi-Ceyhan pipeline. The publication stated that the attacks were carried out from the same addresses as the attacks on the Estonian sites.[9]

CHARACTERISTICS OF CYBERTERRORISM

Today's terrorism is international and, in accordance with a number of international norms, is considered to be an international crime. This is certainly the case for a new manifestation of terrorism — cyberterrorism.

It bears noting that the media often use the term "cyberterrorism" incorrectly, confusing the concept by conflating the terms "hacker" and "cyberterrorist." This, however, is incorrect. Terrorism is a crime, but not every crime is terrorism. Not every hacker commits terrorist acts in cyberspace.

The term "cyberterrorism" was presumably coined in 1997. In that year, FBI special agent Mark Pollitt defined it as "the premeditated politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[10]

Renowned information security expert Dorothy Denning refers to cyberterrorism as "unlawful attacks and threats of attack against computers, networks and information stored therein … to intimidate or coerce a government or its people in furtherance of political or social objectives."[11]

Researchers Matthew Devost, Brian Houghton and Neal Pollard define information terrorism (cyberterrorism being a subcategory) as:

1. The combination of criminal use of information systems via fraud or misuse and physical violence that is characteristic of terrorism.
2. The conscious misuse of digital information systems, networks or components of those systems or networks for purposes that facilitate carrying out terrorist operations or acts.[12]

Three kinds of cyberterrorism can be identified:

1. The commission of terrorist acts using computers and computer networks (terrorism in its "pure form").
2. The use of cyberspace to further the aims of terrorist groups but not directly for the commission of acts of terrorism (on this count former CIA Director George Tenet stated that terrorist groups, including Hezbollah, Hamas, Abu Nidal and al-Qaida are very actively using computer capacities to manage their activities).[13]
3. The commission of acts in cyberspace that do not further political aims but do present a threat to national or public security.

The first kind of cyberterrorism may be defined by combining the concepts of "cyberterrorism" and "cyberspace."

From this it follows that cyberterrorism may be understood as an intentional, politically motivated attack on computer-processed information, a computer system, or a network that jeopardizes the life and well-being of people or involves other serious consequences, if such actions were committed for the purpose of disrupting public safety, intimidating the population or provoking a military conflict. This also includes intimidating the population or government authorities for the furtherance of criminal ends. The latter kind may manifest itself as a threat of violence, maintaining a permanent state of fear in order to achieve political or other ends, coercion, or drawing attention to an individual cyberterrorist or terrorist organization that the cyberterrorist represents. In this case, causing harm or threatening to cause harm serves as something of a warning of the possibility of more serious consequences if the cyberterrorist's conditions are not met.

As for the second kind of cyberterrorism, it may be noted that it is debatable whether the use of cyberspace by a terrorist organization to carry out or publicize its activities but not to commit terrorist acts directly can be regarded as cyberterrorism. Of course, such actions can hardly be qualified as terrorism under criminal law, but nonetheless it seems reasonable to call such actions, cyberterrorism, and apparently this will be done in the near future. This type of cyberterrorism may include such things as:

- Using the Internet to collect detailed information about possible targets, their location and characteristics.
- Creating sites containing detailed information about terrorist movements, their aims and purposes; publishing on those sites information about times and places for meeting people interested in supporting terrorists; information about forms of protest and so forth, that is, synergistically acting upon groups that support terrorists.

THE ASSOCIATED PRESS

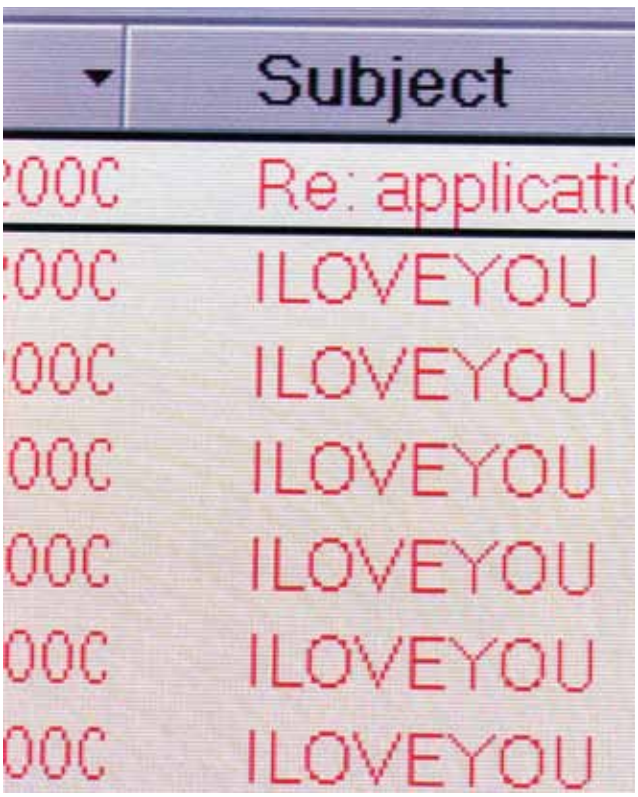
Scottish computer hacker Matthew Anderson appears outside a London courthouse in November 2010. Anderson admitted being a key member of an international gang of hackers who targeted hundreds of businesses with spam.

THE ASSOCIATED PRESS

Briton Gary McKinnon leaves a courtroom in London after facing a hearing for his extradition to the United States in 2005. McKinnon was accused of hacking into U.S. military computers.

- Using the Internet to address a mass audience to report on future or planned actions on the pages of sites or mass e-mailing of similar messages. This includes terrorists using the Internet to publicly claim responsibility for the commission of terrorist acts.
- Using the Internet for informational or psychological effect, including the initiation of "psychological terrorism." The Internet can be used to sow panic, to mislead or for destruction. The World Wide Web provides an abundance of means to spread rumors, including disquieting ones, and this capacity is used by terrorist organizations.
- Raising funds to support terrorist movements.
- Extorting money from financial institutions to spare them from acts of cyberterrorism and damage to their reputation.
- Drawing unsuspecting accomplices into terrorist networks — for example, hackers who do not realize where their actions may ultimately lead. Also, if in the past terrorist networks were usually built around a far-flung structure with a strong center, nowadays they are networks without clearly discernible command points. This is one advantage the Internet provides.
- Setting up Internet sites with a terrorist orientation that contain information about explosives and explosive devices, toxins, and poisonous gases and how to produce them. In the Russian-language segment of the Internet alone there are dozens of sites where one can find such information.
- Using the Internet for communications, and in particular using e-mail or electronic billboard services to send encoded messages. For example, Ramzi Yousef, who organized the bombing of the World Trade Center, received instructions on arranging acts of terrorism via encoded messages sent directly to his laptop. Other terrorist groups, the Black Tigers (a wing of Sri Lanka's defeated separatist Liberation Tigers of Tamil Eelam) for instance, attacked government websites and e-mail addresses.
- Relocating training bases for terrorist operations. Terrorism is no longer confined to the territory of the state in which the terrorists are hiding. Moreover, terrorist training bases are, as a rule, no longer located within the same countries as the terrorists' targets.[14]

As for the third kind of cyberterrorism, actions that may be committed by hooligans and are not aimed at achieving political objectives, but nonetheless may constitute a threat to public and/or national security, can also be regarded as terrorism. This category of cyberterrorism might include intentionally spreading viruses, "Trojan horse" programs, "worms" and so forth, or intruding into and paralyzing the operation of government or other public institutions.



THE ASSOCIATED PRESS

A computer screen in Frankfurt, Germany, shows an e-mail inbox jammed with the powerful "I Love You" virus, which struck global communications systems and crippled government and corporate computer networks in 2000.

THE "I LOVE YOU" VIRUS

A computer virus known as "I Love You" (or the "Love Bug") was launched on the Internet on May 1, 2000, in Asia and spread throughout the planet with astonishing speed. It disrupted the operation of government institutions, parliaments and corporations in many countries, corrupting about 45 million computer networks. For example, in the U.S., this computer virus struck the networks of 14 federal agencies, including the CIA, the Department of Defense, the White House and Congress.[15] It also damaged the British Parliament's network. Altogether, in the first five days after its appearance, it caused material damage totaling $6.7 billion. Thus, it is not surprising that the Computer Economics group assessed the "I Love You" virus as an act of cyberterrorism.

Also in May 2000, Franklin Adams of Houston, in the United States, was convicted of spreading a "worm" that affected computers whose modems were programmed to automatically dial the emergency phone number 911. This resulted in several thousand computers in hospitals, police departments and fire departments being put out of commission, which obviously caused a threat to public security.

An analysis of worldwide trends in the development of cyberterrorism makes it possible to project with a high degree of probability that the threat will continue to increase every year. Technical progress is advancing so swiftly that society is too late to grasp some of its implications, and correcting the situation requires significant effort. In addition, dependence on computer systems and information technologies grows constantly.

Thus, it can be stated that cyberterrorism is a serious threat to humanity, comparable to nuclear, biological and chemical weapons, though because of its recent emergence the degree of the threat is not yet fully recognized and studied. The world community's experience in this area is obvious evidence of the undeniable vulnerability of all countries, especially considering that cyberterrorism does not respect national borders and that a cyberterrorist can threaten information systems located practically anywhere in the world. And finding and neutralizing the cyberterrorist is exceedingly difficult owing to the dearth of clues left behind, in contrast to the real world, where evidence of crime is sometimes easier to collect.

SOLUTIONS IN FIGHTING THE CYBER WAR

All of this requires organizing a broad range of efforts to combat cyberterrorism and cybercrime in general. These efforts may be applied in several areas:

- **Legislative** — Something has been, and continues to be done, in this regard. For instance, national legislatures have adopted specialized laws concerning computer and Internet crime; moreover, legislation in the area of computer crime is becoming a field in and of itself, with ever stricter sanctions against crimes. As time goes by, international legal acts are regulating relations within the Internet and are aimed at countering cybercrime, in particular the European Convention on Cyber Crime. Further refinement of laws, primarily international laws, in the area of combating cybercrime will undoubtedly be a means of fighting this phenomenon.
- **Organizational** — This implies that states organize and cooperate effectively with other states, their law enforcement agencies and special services, and international organizations tasked with combating cyberterrorism and transnational computer crime. There is also a need to create a single international organization, patterned after Interpol, that would exclusively fight cybercrime. A number of countries are already cooperating, but it needs to be expanded and qualitatively improved.
- **Technological** — There is no question that improvements in technologies for protecting society from cybercrimes and responding to them are an important direction in which to move, since this makes it possible to prevent criminals from achieving their objectives, if not from actually committing crimes. Effective partnerships between government institutions and private companies working in high-tech and software development, as well as individual computer technology experts, may help to develop such technologies. This kind of joint effort will enable us to stay ahead of the game rather than being in reaction mode.

All three of the directions outlined above are important and can deliver substantial success in the fight against cybercrime. In principle, some work is being done in these areas. But, paradoxically, implementing these efforts helps to facilitate those very characteristics of cyberspace that make it possible to commit cybercrimes: global reach, accessibility and constant development of technology. However, there is another avenue of action that, in my opinion, is not being given sufficient attention by government bodies. That is decreasing the base of cybercrime, i.e., the number of people who commit cybercrimes. This could be done through focused reorientation of their values. But this area of endeavor requires specific consideration that is beyond the scope of this article.

Today practically any military or political conflict is accompanied by organized opposition on the Internet.

Thus it may be stated that, unfortunately, the development of computer and telecommunications networks, primarily the Internet and the social interactions that arise from it, can be characterized by a constant increase in the number of criminal deeds and other socially dangerous acts in cyberspace. And the high social cost of these acts is primarily due to their transnational nature because the consequences may involve an unlimited number of individuals in the most widespread countries.

Considering this global negative trend, a variety of decisive measures are needed to counter and prevent cyberthreats, bearing in mind the penetration of the Internet and the "virtual world" into all spheres of life. This should become the main thrust of efforts to ensure information security as well as national security in general. □

1. Golubev, V. A., "'Cyberterrorism' – Myth or Reality?" http://www.crime-research.org.
2. Lukatskiy, A. [Лукацкий. А.], "Hackers Are Running the Reactor," Computer Crime Research Center. http://www.crime-research.org/library/Lukac0103.html.
3. Mentor, "Hacker Manifesto," January 8, 1986. http://project.cyberpunk.ru/idb/hacker_manifesto.html.
4. Kurakov, L. P., Smirnov, S. N., Information as an Object of Legal Protection, Moscow: Helios, 1998, p. 220–221.
5. Robert Lemos, "Cyberterrorism: The Real Risk," Computer Crime Research Center. http://www.crime-research.org/library/Robert1.htm.
6. Denning, D., "Activity, Hactivity and Cyberterrorism: The Internet as a Means of Influence on Foreign Policy," Vladivostok Center for the Study of Organized Crime, translated by T. L. Tropina. http://www.crime.vl.ru/index.php?p=1114&more=1&c=1&tb=1&pb=1.
7. Andreyev, A., Davydovich, "On Informational Opposition During the Military Conflict in Kosovo," PSY-FACTOR Center for Practical Psychology. http://www.psyfactor.org/warkosovo.htm.
8. See: http://www.lenta.ru/news/2009/03/12/confess.
9. See: http://www.securitylab.ru/news/384118.php.
10. Rrasavin S., "What is Cyber-terrorism?" http://rr.sans.org/infowar.
11. Denning D. E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." http://www.nautilus.org/ info-policy/ workshop/ papers/ denning.html.
12. Thomas, Timothy L., Deterrence of Asymmetric Terrorist Threats which Society Faces in the Information Age, International Society Against the Globalization of Crime and Terrorism, international conference proceedings, Moscow, 2002, p. 165.
13. Ronald L. Dick, Issue of Intrusions into Government Computer Networks. http://www.fbi.gov/congress/congress01/rondick.htm.
14. Thomas, Timothy L., Deterrence of Asymmetric Terrorist Threats which Society Faces in the Information Age, International Society Against the Globalization of Crime and Terrorism, international conference proceedings, Moscow, 2002.
15. Ronald L. Dick, Issue of Intrusions into Government Computer Networks. http://www.fbi.gov/congress/congress01/rondick.htm.