THE NEW FRONTIER FOR TERRORISTS

By Zahri Yunos

CyberSecurity Malaysia

(This article was published in the STAR In-Tech on 1 Jul 2008)

Introduction

CYBERSPACE is a virtual place that has become as important as physical space for social, economic and political activities. Many nations in the world are increasing their dependency on cyberspace when they use information and communications technology (ICT).

This dependency places countries in a precarious position because cyberspace is borderless and vulnerable to cyber attacks. Individuals have the ability and capability to cause damage to a nation from afar, through cyberspace.

Merely accessing a single personal computer through an Internet connection could cause as much damage as using a traditional weapon, such as a bomb. Cyber attacks are also attractive because it is a cheap weapon in relation to the costs of developing, maintaining and using advanced military hardware.

What is Cyber Terrorism

The term is becoming increasingly common nowadays, and yet a solid definition of it and what constitutes cyber terrorism are subjective and broad.

At first glance, there is nothing new about this term, except for the “cyber” prefix. War, crime and terrorism are traditional concepts that occur in the physical domain; “cyber” refers to the new domain for warfare.

The most widely cited definition of cyber terrorism is by Professor Dorothy E. Denning, director of the Georgetown Institute for Information Assurance, at the Georgetown University in the United States.

According to her: “Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

“Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples.”

“Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not.”

The use of a computer and its applications as a weapon to attack “computers, networks and the information stored therein” constitutes cyber terrorism. There are a number of ways that the terrorist can use a computer as a cyber weapon — computer viruses, hacking, malware, and botnets are a few.

The challenge nowadays is that an attacker’s tools and techniques are becoming more powerful, while requiring less technical knowledge. Furthermore, most of these tools are available on the Internet and at minimal cost, and in some instances, free of charge.

Impacts of Cyber Terrorism

Cyber terrorism is the use of cyberspace to commit terrorist acts. This includes warfare attacks against a nation's state and forcing critical communications channels and information systems infrastructure and assets to fail or to destroy them. These would be:

l. Crippling the electrical distribution grid by shutting down control systems;

2. Disrupting national telecommunications network services;

3. Sabotaging airport traffic control systems;

4. Attacking oil refineries and gas transmission systems by crippling control systems;

5. Destroying or altering banking information on a massive scale, thereby crippling the financial sector;

6. Remotely altering medical information; and,

7. Gaining access to dam control systems in order to cause massive floods.

Why would a cyber terrorist decide to use ICT rather than resort to the usual methods of assassination, hostage-taking and guerrilla warfare?

By using ICT, a handful of cyber terrorists can cause greater damage to a country than an army of a few thousand.

Countries which are increasingly dependent on ICT, especially those that have many systems connected to the Internet, are vulnerable to these kinds of attacks. The paradox is that the more wired a nation is, the more vulnerable it is to cyber attacks.

In an era where the use of ICT is a necessity, it is regrettably also highly vulnerable to attacks and opens a new dimension of threats.

Examples of Cyber Terrorism

It can be argued that cyber terrorism requires political motives and the use of violence. The objective is to create fear within the target population, and monetary gain is not the focus.

One example is the major power failure in the northeast of the United States and Canada on Nov 14, 2003. A power grid is considered one of the major components in a nation’s critical infrastructure. It was reported that hackers

were trying to hit the power system — as many as 100 times a day to compromise the security of the grid.

The incident raised the question of whether it was a cyber attack. Many have worried about the security of control systems in the United States, such as Supervisory Control and Data Acquisition (SCADA) systems that are increasingly being placed online and being opened up to remote access — a move that could contribute to more frequent cyber attacks.

The FBI and the US Homeland Security Department said that the outages appeared to be a natural occurrence and not the result of terrorism. However, Al-Qaeda's group claimed responsibility for the power outage, according to a statement carried by an Arabic newspaper. The truth to this is still not known.

On Aug 4, 2004, it was reported that Japanese Government computers were under attack. Eight government agencies' computer networks were disrupted almost simultaneously. Those networks experienced denial-of-service attacks, and the affected networks were not accessible for a few hours.

Most recently, in May last year, Estonia came under cyber attack for several weeks in the wake of the removal of a Russian World War II memorial. This was a distributed denial-of-service attack that paralysed the Internet communications systems of the government, banks and news media.

Conclusion

Cyber threats are real and no longer limited to the movies. While development in the areas of ICT allows for enormous gains, it has also created opportunities for those who have devious ambitions to cause harm.

We, as a nation, must be prepared for the worst when protecting our critical national information infrastructure. Co-ordination and collaboration from all parties are essential in order to enhance the security of our country in cyberspace.