The Reality of Cyber-Threats Today

Zahri Yunos
CyberSecurity Malaysia
(This article was published in the STAR In-Tech on 23 September 2008)

War, crime and terrorism are traditional concepts that occur in the physical domain. The only difference between those concepts and cyberwar, cybercrime and cyber-terrorism is the "cyber" prefix. Cyberwar refers to warfare in cyberspace and includes cyberattacks against a nation state and critical communication network. Cyber-terrorism refers to the use of cyberspace to commit terrorism. 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 to further political or social objectives. Cybercrime or crime in cyberspace has been much experienced by many parties where the motive is more of computer-related crimes and monetary gain is the focus.

What is a threat?

From the information security perspective, a threat is defined as the potential to cause an unwanted incident in which an asset, system or organisation may be harmed. There are three sources of threats: Intentional, accidental and environmental. Some examples of intentional threats are those that use malicious software or illegal software. Accidental threats can be seen as service failure, human design error or hardware failure. Meanwhile, examples of environmental threats are earthquakes, thunderstorms or lightning. All these threats cannot be totally eliminated, but can be reduced through the establishment of effective measures to curb such threats within each organisation. Threats however, if not properly controlled, can create an unwanted impact on security, socio-economy and human lives.

Cheap method

The dimension of warfare can be categorised as conventional, space and cyber- warfare. Conventional warfare and space warfare are expensive whereas cyber warfare is cheap. It is also accessible to many groups and individuals. Cyber warfare enables asymmetric warfare, where individuals have the abilities and capabilities to cause damage to a nation state. Access to a personal computer with an Internet connection can create as much damage as traditional weapons. It is attractive to many because it is cheap in relation to the cost of developing, maintaining and using advanced military capabilities.

The sophistication of an attacker's tools and techniques is becoming more powerful and requires less technical knowledge nowadays. Furthermore, all of these tools are available on the Internet, which is more user-friendly, at a very minimal cost and in many instances, are free of charge.

There are known threats which have limited capabilities and marginal opportunities with high risks of being detected. There are also emerging threats which have many capabilities and broad opportunities and provide low risks of detection. These are the dilemmas that we face today.

Case studies

Below are several case studies of cyberthreats reported outside Malaysia:

- Cyberattacks experienced by the Japanese government

  It was reported that the Japanese government's computers were under attack on 4 Aug 2004. Eight Japanese government agencies' computer networks were disrupted almost simultaneously, similar to what is known as barrage jamming in telecommunication terms.

  Those networks experienced denial-of-service attacks whereby the affected networks were not accessible for a few hours.

- Hackers clogging up the US customs' computers for hours

  The case was reported in August 2005 where viruses attacked the US Customs and Border Protection system for several hours. Several thousands of people were affected.

  The viruses left a grave impact on the computers at airports in Miami, New York, San Francisco, Los Angeles, Houston and Dallas.

- Cyberattacks on Estonia

  In May 2007, Estonia was under cyberattack for three weeks. The attacks paralysed Internet communications targeting the government, banking, media and police websites.

  Huge economic losses were incurred as online transactions were disrupted.

- Cyber-warfare between Russia and Georgia

  Russia's invasion of Georgia in August had moved into cyberspace as the Russians managed to siege and gain direct routing intended for Georgia.

  It was reported that the Russians intercepted the network traffic to Georgia and redirected the route to their servers. Many of Georgia's Internet servers were under their command and control.

Local attack

In 2001, Malaysia's Internet infrastructure was attacked by the Code Red worm. This was a classic example of infrastructure attack in which the worm spread very fast and brought our national communication network to a standstill. It was reported that the relevant agencies took three months to eradicate this

worm and the estimated minimum losses was RM22mil, not inclusive of the losses to the business fraternity and other sectors as well.

Other incidents of cyberattacks were caused by the Blaster and Naachi worms in 2003. The incident started with the propagation of the Blaster worm through the scanning of vulnerable machines via the network, followed by Naachi worms. These worms exploited the vulnerability found in the Windows NT, 2000 and XP software. The estimated cost to eradicate this worm was about RM31mil, not including lost productivity and the cost of lost opportunity.

Modern warfare

Today, cyberspace is the new war frontier whenever there are conflicts between countries. The popular method of a cyberattack is the defacement of websites. Web defacement is a malicious activity whereby a website is "vandalised". Often the hacker replaces the site's content with a specific political or social message. The hacker may even erase all the contents from the site by relying on known security vulnerabilities to access the site's content. The US-China conflict in May 2001, which resulted from an incident where a Chinese fighter was lost at sea after colliding with a US naval reconnaissance plane, is a good example to illustrate this scenario.

End word

In conclusion, cyber-threats are the problems of today and the future. They need to be addressed in a comprehensive manner. In dealing with cyber threats, a country cannot stand alone. There is a need to have strategic alliances to deal with threats and vulnerabilities in the cyberworld. Coordination and collaboration from all parties is important in order to enhance the security of Malaysia's cyberspace.