PUTTING CYBER TERRORISM INTO CONTEXT

By Zahri Yunos

CyberSecurity Malaysia

(This article was published in the STAR In-Tech on 24 Feb 2009)

A Critical National Information Infrastructure (CNII) is crucial to any nation and the destruction or disruption of its systems and communication networks would significantly effect the economic strength, image, defence and security, public health and safety as well as government capabilities to function. Thus, CNII would probably be the target of terrorists wanting to cripple any country.

The term cyber terrorism is becoming increasingly common nowadays, yet a solid definition for it and what it constitutes is subjective and covers a wide area. Before defining cyber terrorism, it is necessary to define and understand what we mean by terrorism.

What is Terrorism?

Most governments in the world cannot agree on one single definition for terrorism. The ambiguity in the definition brings indistinctness in action; as the old maxim goes “one man’s terrorist is another man’s freedom fighter”.

The US Federal Bureau of Investigation (FBI) defines terrorism as "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

The US Department of State defines terrorism as "premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents".

It is interesting to note that some definitions of terrorism also include targets to computer systems and its services. Australia’s Security Legislation Amendment (Terrorism) Act 2002 defines terrorism, among others, as actions that "seriously interfere with, seriously disrupt, or destroy, an electronic system including, but not limited to, an information system; a telecommunications system; a financial system; a system used for the delivery of essential government services; a system used for, or by, an essential public utility; or a system used for, or by, a transport system."

Malaysia's Penal Code also contains provisions dealing with terrorism. Chapter VIA, section 130B describes terrorism as an act or threat of action within or beyond Malaysia, among others, "designed or intended to disrupt or seriously interfere with, any computer systems or the provision of any services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure".

What is Cyber Terrorism

Part of the problem we face today is in defining cyber terrorism as there are broadly different definitions as to what actually constitutes cyber terrorism. There are a number of well-accepted definitions which have similarities, and there are a number of loose definitions which are promulgated and glamourised by the media.

The term cyber terrorism was first coined in 1997 by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California. He defined cyber terrorism as the convergence of "cybernetics" and "terrorism". Also in the year 1997, Mark Pollitt, a special agent for the FBI, offered this definition of cyber terrorism: "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".

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.”

James A. Lewis, of the US Centre for Strategic and International Studies, has defined cyber terrorism as “the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population”.

Wikipedia defines cyber terrorism as “… subsumed over time to encompass such things as simply defacing a website or server, or attacking non-critical systems, resulting in the term becoming less useful …”. Wikipedia further notes that cyber terrorism requires a political motive and does not primarily focus on monetary gain.

Based on the above observation, the simple definition of cyber terrorism is the use of information technology and its means by terrorist groups and agents. The perpetrator must use information systems or other electronic means to launch the cyber attack.

The traditional terrorism and cyber terrorism share the same attributes. One approach of understanding cyber terrorism is by breaking it down to its fundamental elements. The above definitions suggest that there are at least five elements which must be satisfied to construe cyber terrorism:

- Politically motivated cyber attacks that lead to death or bodily injury;

- Cause fear and/or physical harm through cyber attack techniques;

- Serious attacks against critical information infrastructures such as financial, energy, transportation and government operations;

- Attacks that disrupt non-essential services are not considered as cyber terrorism; and

- Attacks that are not primarily focused on monetary gain.

At the moment, there has been no known publicly reported incident of actual cyber terrorism. Most reported cases are related to cyber threats and the use of the Internet as a tool by terrorists.

Internet as an Ideal Tool for Terrorists

Several works on cyber terrorism and the Internet have been conducted by researchers including experiments on cyber terrorism activities on major websites and blogs such as YouTube and Second Life. The researchers also studied popular hosting service providers such as blogspot.com and wordpress.com. Their findings indicate that:

- There have been several cases reported in the media where the Internet has helped terrorists in their cyber activities.
- The virtual world is indeed used to promote cyber terrorism activities. Some of the videos published on the Net are related to explosives, attacks, bombing and hostage-taking.
- Some terrorist groups use the Internet for the purpose of inter-group communication and inter-networked grouping.
- The Internet is used to release manifestos and propaganda statements.
- Aside from generating propaganda, the Net is also used to coordinate missions or call meetings and to recruit new members.

Conclusion

This article provides an overview of the definitions of traditional terrorism and cyber terrorism. There is a broad range of differing opinions as to what actually constitutes cyber terrorism. As long as the term continues to be used without a proper understanding of the nature of cyber terrorism threats, the misinformation and hype associated with it will remain.

There are reported claims that cyber terrorists use the Internet as a medium for hostile activities. It is imperative that an explanatory study of cyber terrorism activities on the Internet be conducted. Future studies in this area perhaps can provide a better understanding of the ideas and communication patterns of cyber terrorists, which may lead to the development of strategy and policy framework to counter cyber terrorism.

Disclaimer:

(Zahri Yunos is the Chief Operating Officer of CyberSecurity Malaysia. The views expressed here are his personal views.)