International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:1, No:6, 2007

Status and Requirements of Counter-Cyberterrorism

Jeong-Tae Kim, and Tchanghee Hyun

***Abstract*—**The number of intrusions and attacks against critical infrastructures and other information networks is increasing rapidly. While there is no identified evidence that terrorist organizations are currently planning a coordinated attack against the vulnerabilities of computer systems and network connected to critical infrastructure, and origins of the indiscriminate cyber attacks that infect computers on network remain largely unknown. The growing trend toward the use of more automated and menacing attack tools has also overwhelmed some of the current methodologies used for tracking cyber attacks. There is an ample possibility that this kind of cyber attacks can be transform to cyberterrorism caused by illegal purposes. Cyberterrorism is a matter of vital importance to national welfare. Therefore, each countries and organizations have to take a proper measure to meet the situation and consider effective legislation about cyberterrorism.

***Keywords*—**Cyberterrorism, cyber attack, information security, legislation

I. Introduction

THE advances in information technology have a large effect of our life and society. A greater part of our activities has come to depend heavily on communication infrastructure. This dependence on information technology has created a new form of vulnerability for our life can be greatly harassed by those who can connect to network and deal with information technology for social or political purposes. Information technology can be handled by criminals and terrorists to pursue their malicious intents.

After several physical terror attacks such as the September 11 terror attacks on the World Trade Center and Pentagon, the potential threat of cyberterrorism also has increased gradually. Cyberterrorism against critical infrastructures such as transportation, electric power grid, oil and gas distribution, telecommunications, and finance are recognized as important. Thereby, some governments and international organizations are making an effort to ready countermeasures against cyber-terrorism. But, countermeasures that several countries are establishing hastily after September 11 terror attack are somewhat short of logic and system. If we try to look for technological solutions without considering the difference between physical terrorism and cyberterrorism has, they may have some fatal defect.

Jeong-Tae Kim is with the Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea. (phone: +82-42-860-1172; fax: +82-42-860-6504; e-mail: acroo@etri.re.kr).

Tchanghee Hyun is with the Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea (e-mail: chhyun@etri.re.kr).

The damage of cyberterror attacks can spread to unpredicted amount or level. Therefore, it is desirable that get into situation that cyberterrorism should be considered significantly in a conception of the national security. As the national security became much harder to estimate, we must prescribe primary factors which make threats to the national security and complete proper counter-cyberterrorism plans.

It is difficult to catch the subject of terror and takes long time to grasp the starting point in the case of terror through network and determine the level of countermeasure because the subject of terror is ambiguous if it is a recreational hacker or regular army raised by a particular group or a country. And it is not simple to decide to counterattack or not when the subject of terror is revealed because it is not certain if the terror is related with international law or if physical retaliation is tolerated for the cyberterror. There are numerous types of cyberterror and sizes of damage, so accurate rules have to be laid down.

II. An Overview of Cyberterrirosm

A considerable percentage of our life has come to depend heavily on information technology or network. As dependency on computer systems and network increases in many countries in 1990s, many experts begin to estimate that computer systems and network can be a new objective of attack from certain groups or countries. This kind of concern has been amplified progressively after the point of time that the September 11 terror attacks happened. The vagueness of cyberterrorism conception stimulates people to worry and distorts nature of the conception. It is very important to prescribe cyberterrorism to avoid distortion of the conception. All attacks against certain objective through network are not cyberterror. It should be considered that the objective of cyberterror is threatening critical infrastructure connected to network besides objective of cyber crime is private benefit. In recent times, Internet worms and network viruses often threaten international network system. This kind of malicious codes is not more than personal naughtiness or a small crime. But if these events tent to make threats objective of terror by certain group or country, it can have a critical impact on national security.

The US Federal Bureau of Investigation (FBI) defines cyberterrorism as, cyberterrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant objectives by sub-national groups or clandestine agents [13].

There is a representative definition of cyberterrorism proposed by National Infrastructure Protection Center (NIPC)

that cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction andor disruption of services to create fear by causing confusion and uncertainty within a given population, with the objective of influencing a government to conform to a particular political, social, or ideological agenda [6].

A specialist in cyberterrorism, Dorothy Denning, defines cyberterrorism as, 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 cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear [4].

Conventional terrorists might see greater potential for cyberterrorism than the existing terrorists, and their level of knowledge and skill relating to hacking will be greater. Hackers and insiders might be recruited by terrorists or become self-recruiting cyberterrorists. Some might be moved to action by cyber policy issues, making cyberspace an attractive venue for carrying out an attack. Cyberterrorism could also become more attractive as the real and virtual worlds become more closely coupled, with a greater number of physical devices attached to network.

There are various advantages that attract terrorists to pick cyberterror. It starts with the benefit of cost. Terrorists, generally suffered from being short of funds, do not have to get an expensive conventional weapons and convey them to the intended site. They can achieve terror attack by just transmission malicious codes they created. Cyberterrorism has a superior level of anonymity than the conventional terrorism. Anonymity is a common characteristic of computer network. Therefore, Identifying and tracking terrorist is very tricky by using the log information of cyber attack. Cyberterrorists are not limited by time or space. The terrorist could even be half way around the world at any time. Cyberterrorism have more power of influence than conventional terror attack. Internet worms they created are able to make threats millions of people within few hours and cause massive amount of damage. In the computer dependent society, the potential objectives of attack are incalculable. Finally, there are a numerous ways that cyberterrorists can use the computer as the tool of attack as well. Logic bombs, Trojan horses, worms, viruses, denial of service, and other information warfare tools are now the munitions store in a new geopolitical calculus whereby foes can take on a superpower that can no longer be challenged with conventional weapons.

III. Status of Counter-Cyberterrorism

A. Countermeasures of International Organizations

Each advanced countries make an effort to decrease the damage of cyber attacks to domestic area from technological ways. On the contrary, a number of international organizations are managing politic countermeasures against cope with cyber attacks. This behavior came from the agreement in view and judgment that cyberterrorism is a global question, not a domestic thing.

The Council of Europe (EC) introduced guidelines on cyber crime in 1998. This guideline outlines a policy to counter computer crime and terrorism and describes the mechanisms necessary to achieve this without hindering rapid development of e-commerce in the EU or affecting citizens' fundamental right to privacy. The guideline demands a number of legislative and non-legislative actions. Legislative proposals include harmonizing member states' laws. Non-legislative action proposed in the guideline includes the creation of an EU Forum to raise public awareness and promote best practices in IT security. The forum will bring together representatives from law enforcement agencies, service providers, network operators and data protection authorities.

To enhance and supplement conventional methods of obtaining assistance in cases involving networked communications and other related technologies, the G8 created 24/7 Network by which participating countries designate a point of contact for cyber incidents that can be available to assist 24 hours a day, 7 days a week. This network has been used in many instances to investigate threats and other crimes in a number of countries. The network has also been used on several occasions to avert hacking attacks, including attacks on banks worldwide.

The Organization for Economic Cooperation and Development (OECD) has released its Guidelines for the Security of Information Systems and Networks. These Guidelines consist of nine principles that aim to increase public awareness, educations, information sharing and training that can lead to a better understanding of online security and the adoption of best practices. The nine principles of the newly announced Security Guidelines include: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, reassessment. The Guidelines encourage governments in other countries to adopt a similar approach and ask businesses to factor security into the design and use of their systems and networks and provide security information and updates to users. The Guidelines urge all individual users to be aware and responsible and take preventive measures to lessen the security risks inherent in an interconnected world.

Asia-Pacific Economic Cooperation (APEC) has taken a lead within the Asia-Pacific region to promote cyber security and address the threats posed by cyber crimes and terrorism. In their Statement on Fighting Terrorism and Promoting Growth, APEC Leaders collectively committed to: endeavor to enact a comprehensive set of laws relating to cyber security and cyber crime that are consistent with the provisions of international legal instruments and identify national cyber crime units and international high-technology assistance points of contact and create such capabilities to the extent. Moreover, the APEC Cyber Security Strategy recognizes the need for the development and maintenance of law enforcement units dedicated to fighting cyber crime. It mandates APEC work to

assist member economies to develop law enforcement units capable of international cooperation in computer crime investigations. This strategy has six areas about: legal developments, information sharing and cooperation, security and technical guidelines, public awareness, training and education, wireless security.

B. Countermeasures in the United States

The terrorist attacks of September 11, 2001 are said to have "completely changed the mind of national security." The existing national security strategies have been re-evaluated and new strategies for the cyber space have been created. The US, The developed country in IT field, is badly damaged by the intrusions and cyber attacks to the system of critical infrastructures or military installations. Therefore, cyberterrorism threats become more realistic. For the reduction of threats to national security, US seek to establish several laws and strategies like followings.

-- Cyber Security Enhancement Act of 2002, H.R.3482 (adopted on May 8, 2002)

-- The National Strategy to Secure Cyberspace (released on February 14, 2003)

Passed by the House and the Senate, Cyber Security Enhancement Act as amendments of Homeland Security Act calls for an effort to toughen the authority of federal government for securing the national infrastructures and computer systems. Under the act, federal agencies are able to eavesdrop the personal e-mails and other electronic telecommunication ways and the punishment of the crime of illegal accessing to the computer systems of federal governments.

After the legislation of The National Strategy to Secure Cyberspace (NSSC) strategy, National Cyber Security Division (NCSD) established. The role of NCSD is detection and removal of the security hole of national infrastructure and illegal events that happens on the network, tracing subliminal threats on the cyber space, cooperation with similar agencies and information sharing. The US National Infrastructure Protection Center (NIPC), transferred to the Department of Homeland Security (DHS) under the NSSC strategy, gain access to information that enables them to protect their assets and give information to the government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The Department of Justice (DOJ) has been developing professional knowledge about how to handle illegal computer crimes. DOJ established several small agencies such as CCIPS, CTC, CHIP and is developing legal advices or interpretations and technology that is securing electronic evidences.

C. Countermeasures in Japan

Japanese government established the advanced IT society and e-government (e-Japan) through the 'e-Japan Strategy'. After the illegal intrusion to servers of several government agencies, attacks to web site of some newspaper offices and enormous trial of accessed from Korea about the revision of authorized middle school history textbooks and the visiting war shrine, The Japanese government has decided upon a positive countermeasure policy to cyberterrorism. Up to the present, Japanese government passed some cyberterrorism policies as followings.

--Action Plan for Information Systems Protection against Cyber-threats (adopted on January 21, 2000).

--Guidelines for IT Security Policy (formulated on July 18, 2000).

--Special Action Plan on Countermeasures against Cyber-terrorism of Critical Infrastructure (adopted on December 15, 2000).

--Comprehensive Strategy on Information Security (announced on October 10, 2003).

The Action Plan outlined the constructing a governmental structure to respond to cyber threats, the establishing IT security policy and the developing cyberterrorism countermeasures against protect critical infrastructure. The Guidelines for IT Security Policy work as a reference manual for the ministries and agencies in drawing-up the Policy and indicates the minimum measures that each ministry and agency should provide. After the adoption of several action plans, Ministry of Economy, Trade and Industry (METI) passed Comprehensive Strategy on Information Security. Based on Cyberterror Countermeasure plan of this strategy, Cabinet Secretariat (CS) has been developing the service supporting system for information security countermeasure and the database of terror countermeasure. CS begin National Incident Response Team (NIRT) within the IT Security Office to carry out investigations and advising required by ministries and agencies to formulate IT security measures with respect to incidents related to IT security, such as cyberterrorism. National Police Agency established Cyber Force, the special unit to deal with technological aspects of counter-cyberterrorism. This unit is in charge of monitoring and emergency response to attacks to police's network and social infrastructure.

IV. Requirements for Counter-Cyberterrorism

Counter-cyberterrorism plans that some developed countries and international organizations planned are composed of preparations of information security technology to avoid occurrence of terrors and precautions such as toughening the punishment on terrors, forming an organization to cope with terrors and promoting international cooperation.

But, when a cyberterror takes place between groups or countries actually, there is not a consideration about how to do substantial countermeasures like punishment or reprisal attack to the cyberterror. If groups who attack and are attacked are under the different jurisdiction, controversy is expected over which criteria are used to make a decision and to counter. For the existing treaties for cyberterrorism, it must be considered facts as follows [10].

-- Countermeasure against the mixed attack of cyber and

physical terrors

-- Countermeasure according to subject of an attack

-- Interpretation criteria for deciding the beginning of an attack

-- Decision criteria for the place where attacks take place

-- Determination criteria of countermeasure against terrors

The existing countermeasures are based on the assumption that a cyberterror takes place independently and individually. But, there is an ample possibility that the cyberterror takes place connected with a physical terror by a group or a nation. On the occasion of concurrent occurrence of physical and cyberterror, we have a need of criteria for selection of countermeasure whether we divide two terrors as another question or hold two terrors together in one category.

Decisions that what action should be taken are made according as the subject who attacks is individual or country. If the subject is individual, general or demonstrative punishments should be suffered. If the subject is country, reprisal actions should be taken. It requires that systemic examinations are completed whether we regard an individual terror behavior as a national action or see them separately. After the terror attack by hostile country, it requires criteria for classification of combatants into a regular army or not. Unlike the conventional terrorist who has characteristic of bearing arms, there is nothing about cyberterrorists which distinguishes them from civilians.

If we regard a cyberterror as a kind of a physical attack, a standard of judgment that when the attack has been made and a state of open hostilities began to emerge is needed. Generally, cyberterror attacks have no definite marks of the beginning of attacks. Therefore, some countries related to terrors may raise an objection to the beginning.

In the case of cyberterrorism, locations where attacker located and attack takes place could be under the different jurisdiction. Therefore, a standard of judgment that which country the subject of attacks belongs to is needed. If the country where attacks take place should treat the cyber attack as a kind of a physical attack at their discretion and decide to do a retaliatory act with military force, there will be a serous conflict with the country that has different criteria.

V. Conclusion

An actual cyberterror attack has not occurred yet by this time. In spite of the frightful scenes of terrorism that have occurred in the last few years, it appears that none of them classified into cyberterrorism causing loss of life or serious social and economic damage. However, we could all agree that there have been many instances of attacks on several infrastructures through network that have gave rise to social and economic suffering and one successful cyberterror attack can cause critical destruction.

Cyberterrorism can not be avoided by developing an information security technology and concluding treaties about cyberterrorism between allied nations. Terrorists are able to intrude into a system connected to critical infrastructure through the most vulnerable node among numerous nodes of allied nations. Therefore, it is essential that all of the governments continue to make narrow the technological gap about the information security and cyberterrorism and to seek the technological cooperation about the information security. In the aspect of legal adjustment, we have to realize the difficulty that the existing law about physical terrorism can not be applied to IT environment these days and have to systemize the characteristics of cyberterrorism.

Regardless of various countermeasures of each nation about cyberterrorism, new elements of threat can appear, because IT environment is developing itself. The more successful countermeasures are, the more enthusiastic terrorists will search for new vulnerable objectives. Thereby, we have to set up countermeasures for a various fields and should take special precautions to avoid cyberterrorism.

References

[1] Borchgrave, A., William H.W. "*Cybercrime, Cyberterrorism, Cyber warfare*", CSIS Publications, 1998
[2] Cameron, J., Vaile, D. "*The War on Terrorism Vs. Cyber Liberties*", IFIP WG, 2003
[3] Cordesman, A.H. "*Cyber-Threats, Information Warfare, and Critical Infrastructure Protection*", CSIS, 2002
[4] Denning, D.E. "*Cyberterrorism*", Global Dialogue, 2000
[5] Department of Defense, Office of General Counsel, "*An Assessment of International Legal Issues in Information Operations*", 1991
[6] Garrison, L and Grand, M. "*Cyberterrorism: An evolving concept*", NIPC Highlights, 2001
[7] Goodin, D. (1997) "*Taking Aim at Cyberterrorism*," Available: http://news.com.com/2100-1023-204515.html
[8] Grossman, M. (1999) "*Cyberterrorism*", Available: http://www.mgrossmanlaw.com/articles /1999/cyberterrorism.htm
[9] Jalil, S.A. "*Countering Cyberterrorism Effectively: Are We Ready To Rumble?*", SANS Institute, 2003
[10] Kim, J. T., Park, S. Y. and Hyun, T. (2005) "*An Inquiry into International Countermeasures against Cyberterrorism*", ICACT 2005
[11] Mitliaga, V. (2001) "*Cyber-Terrorism: A Call for Governmental Action?*", Available: http://www.bileta.ac.uk/01papers/mitliaga.html
[12] Nagpal, R. "*Cyberterrorism in the Context of Globalization*," National Seminar on "Globalization and Human Rights", 2002
[13] Pollitt, M.M. (2003) "*Cyberterrorism - Fact or Fancy?*", FBI Laboratory, Available: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html