Data Protection and the Proper Response to the Cyber Crime : The Two Common Goals

Jaeyoung LEE
Prosecutor, National Security Department
Seoul Central District Prosecutors' Office
ROK

1. Introduction : July 2009 Cyber Attacks

As everybody knows, in early July 2009, there were a series of coordinated cyber attacks against major government, news media and financial websites in South Korea and the United States. The attacks involved a large number of hijacked computers, known as a DDos attack. Most of the hijacked computers were located in South Korea.

The attacks were continued from July 4. to July 9. in three phases. Among the websites affected were those of the White House, Blue House, the Pentagon, the Ministry of Defense of Korea, the National Intelligence Service and the National Assembly.

2. The need to defend cyber crime

It would be better to begin with the Internet infrastructure in Korea.
By June 2007, according to the official statistics, the number of Internet subscribers in Korea is more than 34 million which means that 75% of Koreans are using Internet. Especially, in the aspect of subscription to the super-highway information network, 90% of Korean families are subscribing to the super-highway Internet network system.

As we all know, Korea has one of the highest developed Internet network in the world. The ITU, International Telecommunication Union, put Korea in the first place of DOI, that's to say Digital Opportunity Index, among one hundred and eighty countries which are evaluated by means of Internet infrastructure, chances to the Internet service, and availability. For example, Korean people are using Internet banking service for checking an account, transferring money and taking out a loan over 17 million times in a day.

However, the high-speed development of the Internet in Korea results in a major problem of protecting the security of the network and information on Internet. There were some cases showing the vulnerabilities in Korean cyber space. In April 26th, 1999, over 1 million of Korean computers which means 13% of domestic computers were infected by CIH virus and it cost 40 million dollars to repair them. There was another Internet disaster in January 25th, 2003. At that time, almost all Korean Internet network was paralyzed for 13 hours by Slammer Worm virus. From above incident, we can easily recognize the vulnerabilities of Korean cyber space to certain cyber attacks.

It is not only in Korea that the information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those functions now depend on an interdependent network of critical information infrastructures. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.

In recent years, large amount of information security incidents have caused a great lost to many countries, and the occurrence of such incidents is now on the rise, indicating that information system and network have become the major targets in future war and conflict.

This stresses the need for cooperation between governments and the private sectors and international cooperation in identifying, preventing, and mitigating cyber-attacks and terrorist misuse of cyber space.

3. Legislation that covers cyber crime in Korea

Korean government pays high attention to the cyber crime and has taken the effective measures on legislation, security of network and fighting cyber-crime etc.

Most of criminal activities can be covered by general criminal law which includes the interruption of business, deletion of data, illegal intrusion into the network, and forgery of public record by means of cyber attacks such as hacking. If there are some kinds of wrongdoings to the hardware, general criminal law would be also applied.

Moreover, two special law articles can be mentioned as main legislative countermeasures against cyber-crime and cyber-terrorism.

First, "Act on Promotion of Information and Communication Network Utilization and Information Protection" covers several types of crimes involving cyber-crime. Specifically, the Act provides that anyone who distributes computer viruses or malicious code shall be sentenced not more than 5 years in jail or fines not more than 50 thousand dollars. Same amount of sentence will be provided to anyone who brings about damages to information network with some kind of illegal activity such as Distributed Denial of Services. Additionally, the Act prescribes that anyone who infringe on the network without proper authority or by exceeding his authority will be sentenced not more than 3 years in jail or fines not more than 30 thousand dollars.

Second, "Act on Information and Communication Infrastructure Protection" raise the punishment of above unlawful act when it brings about damages to information and communication infrastructure. According to the Act, anyone who causes damages to critical network infrastructures related to national security or economic transactions shall be sentenced not more than 10 years in jail or fines not more than a hundred thousand dollars.

4. The investigative system in korean prosecutors' office

To begin with, Korean prosecutors' office did not have enough opportunity to handle terrorism cases. It might be great fortune for our country but it makes us rather inexperienced for that kind of attack. Secondly, in terms of technology, Korean prosecutors' office is not so advanced as the other government investigative bodies such as police department and National Intelligence Service.

The core national institutions for cyber-crime(including cyber-terrorism) are the National Cyber Security Strategy Council and the National Cyber Security Committee under the council. In January 2005, the Council was organized in the National Intelligence Service by National Cyber Security Management Regulations. The chief of NIS is to be the chairperson of the Council and the vice-chief of relevant authorities such as Ministry of Justice, Ministry of National Defense and others participate as a member of the Council. The Council establishes and improves national cyber security system and coordinates the function of each relevant authority. In addition, the Council administers the National Cyber Security Committee under its influence.

The response system against cyber-terrorism in Korea can be divided into three parts.

The first part of the system is gathering and distributing terrorism information. Also, in Korea, establishment of proper countermeasures will be done in this part. Concerning cyber-terrorism, National Cyber Security Center in NIS plays a main role in processing the relevant information.

Secondly, government in both the state and local level do research and support, in case there is certain kind of terrorism threat or there are cyber crimes involving terrorism.

Lastly, prosecutors' office and police department investigate the cyber-terrorism cases once there occurs some criminal activities.

Of course, each part cooperates with each other in systematic manner for effective response measures. They share cyber threat information with each other during normal times and prevent attack incidents. In the case of a cyber attack incident, they get real time consultation on countermeasures and minimize the damages. After some kind of terrorism activity, they exchange their information to pinpoint criminals through cooperative investigation among each government officials.

As we all know, electronic crimes are not traditional crimes in form and nature, therefore, a highly trained and specialized agency for the purpose of investigation and prosecution of the criminals should be designated for this job. This is important because not only the natures of crimes are technical in nature but the investigation procedures are also highly technical and different for the investigation procedures of conventional crimes.

Among divisions in our prosecutors' office, national security division and high-tech crime investigation division are in charge of cyber-terrorism cases. Cooperative system is inevitable because cyber-terrorism has both the aspect of terrorism and cyber crime.

5. Cyber Attacks without boundary : The need to cooperate internationally

We can respond to the cyber crime effectively only through international cooperation, taking into account the fact that high-speed internet networks were spread around the world and attacks are disguised through a stop-over at 3rd country.

As we all know, the largest threat associated with cyber terrorism is the "detached" nature of attacks. Borders do not have to be crossed, bombs do not have to be smuggled and placed, hostages do not have to be captured, terrorists do not have to surrender their lives.

Terrorists may be able to do more with a keyboard than with a bomb. Attackers could wage cyber warfare from a computer anywhere in the world, undetected. Terrorists can use the Internet to communicate with each other to plan and coordinate attacks. Many terrorist groups even maintain their own websites.

So, we must take steps to build a strong network to fight against cyber crimes.
First, we should share cyber threat information with each other during ordinary times and preventing attack incidents.
Second, in the case of a cyber attack incident, real time consultation on countermeasures and minimization of damage will be needed.
Third, we would only be able to pinpoint hackers through cooperative investigation among each country's law enforcement.

It is said that the problem was made worse by increased connectivity between countries, but the network will facilitate the real-time exchange of threat and vulnerability assessment and issuance of required warnings and patches.

6. Conclusion

In Korea, we have quite an elaborate legal response system against cyber-crime in our own way. However, such system still has to be improved in order to combat the rapidly developing crimes in cyber space more successfully. It is obvious that exchanging of views and best practices among international prosecutors working in the same field, the fruits from the discussion shall be very useful for the development of each country's response against cyber-crime.

We should stress the need for cooperation between governments and the private sector in identifying, preventing, and mitigating cyber-attacks and terrorist misuse of cyber-space.

I believe that an effective fight against cyber-crimes requires increased, rapid and well-functioning regional and international cooperation.