4

Cyber Security Measures
—How to protect the nation's critical infrastructure from cyber attacks—

Tomoe Kiyosada, *Information and Communications Research Unit*
Hajime Yamada, *Affiliated fellow*

4.1 Introduction

The terrorist attacks on September 11, 2001, targeting the U.S., have driven not only the country but also the world into turmoil. Terrorism carried out by only a few tens of people caused a major disaster involving thousands of casualties, which resulted in chaos in the city for several days.

Under U.S.-lead retaliatory strikes, the possibility of further counter-attacks by terrorists is posing a greater threat to us. What type of measures would they take? What can our government do to prevent damage?

By focusing on cyber terrorism, this report provides information on how the U.S. has been developing cyber security policies from an early stage, which will contribute to our policymaking to improve cyber security.

4.2 Cyber Attack Threat

4.2.1 Will there be further retaliatory attacks?

On October 11, the Federal Bureau of Investigation (FBI) officially warned that there was a probability of additional terrorist attacks within a few days ("Immediate Release," FBI National Press Office). The Washington Post also reported on October 5 that officials from the FBI, CIA (Central Intelligence Agency) and DIA (Defense Intelligence Agency) unofficially stated to the members of the Senate and House Intelligence Committees, "there is a 100 percent chance of an attack should the United States strike Afghanistan." ("FBI, CIA warn Congress of more attacks as Blair details case against Bin Laden," Washington Post.)

4.2.2 Further retaliation through cyber attacks

Assuming terrorists are planning retaliations, what measures would they take? Taking their presumably scarce resources into account, they are likely to use biological, chemical or cyber weapons, which can be developed and executed with limited labor and cost, instead of missiles for armed attacks.

Actually, in the U.S., anthrax infected patients turned up one after another, increasing the threat of bio-terrorism. However, as security against terrorism becomes extremely tight throughout the country, cyber attacks, which can be carried out from a remote place, are no less serious a threat than bio-attacks. In fact, Infrastructure Defense (iDEFENSE), an information provider dedicated to cyber security, pointed out that supporters of either terrorism or anti-terrorism have already organized hacker groups, through which cyber attacks have started against targeted Web sites such as those operated by U.S. corporations or by Islamic nations (iDEFENSE Report #105540, #105551).

4.2.3 Terrorists' capability of cyber attacks

Next, how terrorists are capable of cyber attacks is discussed.

It is reported that Bin Laden is likely to have been secretly sending instructions for attacks by using a technology known as steganography ("Terror groups hide behind Web encryption," February 6, 2001, USA TODAY).

Steganography is the technique of embedding secret messages, images, or data in ordinary file formats sent over or displayed on the Internet such as texts, images, and audio. Professor Johnson, George Mason University shows on his

Web site (http://www.jjtc.com/stegdoc/sec313.html) the comparison of an image with data embedded by using steganography and the same image without the hidden data. There is virtually no visible difference between the two. Secret information is typically sent by using an encryption technique, and thus it is clearly known something is hidden within the encrypted data. On the other hand, steganography does not allow others to readily recognize if there is masked information or not, thus enhancing confidentiality. In addition, while encrypted data is often detected by data traffic interception systems online, this is not likely to occur with steganographic data.

Dr. Hunker, who led the cyber security division of the National Security Council (NSC) under the Clinton administration, pointed out that the September 11 attacks must have been well-prepared by well-educated people probably with abundant financial resources. He also said if these people had carried out a cyber attack, the result would have caused as great damage to the U.S. ("U.S. Networks Run Big Risk of Cyber-strikes," Experts Assert, October 3, 2001, Mercury News.)

The above chapter showed an analysis of; i) Cyber attack threat, and ii) Terrorists' capability of cyber attacks. With attention to how the U.S. developed their cyber security policies from an early stage, the following chapters outline the policies as well as the background that made the country address this field.

4.3 Enhanced Cyber Security Awareness in the U.S.

Development of information technology (IT) facilitated the connection of the critical infrastructure of defense, electricity, natural gas, telephone networks, and transportation to the Internet. While improving convenience, this has increased the vulnerability of these systems. Meanwhile, there has been a growing number of unauthorized entries into key infrastructure systems in the U.S. over the past few years ("Emerging Challenge: Security and Safety in Cyberspace," Ver. 14, No. 4, Winter 1995-1996, IEEE Technology and Society Magazine). Thus, cyber strikes on critical infrastructure are being recognized as a new national security threat.

4.3.1 Exercises assuming cyber attacks

On March 23, 1996, the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense (DOD) conducted an exercise called "The Day After...," assuming a variety of damage that could be caused by a cyber attack targeting key infrastructure (Strategic information warfare: a new face of war," Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, Rand Corporation). The cyber strike scenario developed for the exercise is described in Table 1.

Now that a terror attack beyond our imagination occurred, the cyber strikes described in the above scenario sound more realistic. The following section outlines an experiment conducted to examine the feasibility of such cyber attacks.

4.3.2 Computer system vulnerability study

In June 1997, DOD conducted an experiment called "Eligible Receiver" to examine the vulnerability of DOD key infrastructure, such as networks, communications systems, and the power grid, against cyber attacks (Testimony by Mr. Richard C. Schaeffer, Jr., October 6, 1999, Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information). For this experimental exercise, 30 officials at national security organizations acted as hackers with the following mission.

— Shutting down the control systems for key infrastructure such as communications networks and the power grid.

— Entering DOD computer networks without authorization.

The participants were also told; i) while simulating an attack on key infrastructure, they should leave a sigh in the system they penetrated, instead of actually shutting down the system, and ii) with respect to the unauthorized access experiment, they should clearly indicate how deep they penetrated.

The acting hackers followed these terms:

— Do not use knowledge obtained through their jobs.

— Buy and use any computers available off the

Table 1: Cyber strike scenario

Date and Time (EDT)	Proceedings
Evening, May 11	NCC reports to the White House that; (1) the public telephone network system for Northern California and Oregon suffered a failure due to a Trojan horse, and (2) the base phone system for Fort Lewis had been subjected to a DoS attack and their communications system had been paralyzed for several hours.
Later at night, May 11	In Cairo, Egypt, the electricity supply system failed, leaving 90% of the nation's households without power for several hours.
4:00, May 13	A large oil refinery in Southeast Sandi Arabia suffered a control system failure, causing an explosion and fire.
18:12, May 14	In Maryland, a logic bomb embedded in the transportation system network exploded, causing a collision between a freight train and a high-speed train. Maryland State Police estimate 60 dead and 120 injured.
6:00, May 16	Scotland Yard reports to the British Prime Minister that the Bank of England detected three failures in their funds transfer system and the Bank leaders, considering this serious, suspended the funds transfer service.
Morning, May 20	Joint Chiefs of Staff (JCS) information warfare planning cell announced that their computer program for time phased execution control is infected with an unknown worm.
12:10, May 20	The automatic tellers of the two major banks in Georgia started to malfunction causing a bank run. These banks were forced to shut down their ATM systems.
12:25, May 20	The CNN news center feed out of Atlanta was off the air for 12 minutes.
15:30, May 20	CNN aired a special report focusing on the vulnerability of the U.S. to cyberspace warfare, dwelling on the series of incidents including; (1) the crash of the express train linking Boston, New York and Washington D.C., (2) the telephone outage in the Northwest, (3) the malfunction of the ATM systems in Atlanta, and (4) the still-unexplained interference with CNN's signal transmission.
Evening, May 20	Local and national evening programs reported that U.S. military deployments to the Gulf were experiencing delays due to cyber attacks on the LANs and phone systems of key Army and Marine bases.
19:44, May 22	The pilot of a Continental Airline's Airbus-340 making a final approach to O'Hare International Airport reported to the control tower that his flight deck avionics had suffered a malfunction and that the aircraft was out of control.
Night, May 22	After receiving a preliminary British report concluding that all late model AB-330 and 340 flight control software may be infected by a sophisticated logic bomb, the administrator of the FAA recommended that all late model AB-330s and AB-340s be immediately grounded until the nature of the flight deck malfunction can be ascertained.
12:57, May 23	The Saudi public switched network began to fail apparently due to unauthorized modification of the system through trap doors.
16:10, May 23	The Secretary of Defense was informed by the JCS Chief that a full-scale IW attack by unknown sources was underway at almost every military base in the U.S. and Europe.
19:00, May 23	Several radar aircraft operating in the Gulf region were plagued with a computer worm.
10:30, May 24	The entire phone network system in the Washington/Baltimore region including local cellular systems failed due to trap doors.
13:30, May 24	The Chicago Commodity Exchange experienced some of its wildest fluctuations in history. There was widespread suspicion that the Exchange was being subjected to a form of electronic manipulation by parties unknown.
Afternoon, May 24	In Washington D.C., an emergency NSC meeting was called by the President but the arrangement was difficult because of the phone system shutdown.

Notes:
NCC: National Communications Center
Trojan horse: A program set on a computer system that allows the program developer to take control of the system.
Trap door: A technique that permits designated third parties to access a targeted program or network, bypassing passwords or other security procedures.

Source: "Strategic information warfare: a new face of war," Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, Rand Corporation shelf.

— Carry out an attack over a commercial Internet service.

— Use hacking tools available and downloadable from Web sites.

Prior to the exercise, the participants had a three-month preliminary period. During the exercise, they gained unauthorized access to key infrastructure and left signs showing their ability to turn off the systems. They also successfully broke into DOD computer networks. There were 40,000 attempts of unauthorized access to the networks, out of which 36 were successful. However, it was only two of them that DOD system administrators could detect. Some hackers even succeeded in obtaining a system administrator's authority, which allowed them to access any desired DOD network.

This experiment showed that as few as 30 people who do not have any special skills could have paralyzed critical communications networks and the power grid, and could have taken control of DOD networks, which are protected with one of the most sophisticated security systems in the world. In other words, it was proven that a small number of people could cause a national security crisis in the U.S. The result shook the U.S. government so violently that the government officials could not help starting to seriously address cyber security issues.

4.4 Critical Infrastructure Protection in the U.S.

The critical infrastructure protection policy the federal government is now working on is based on the scheme announced by then- President Clinton in January 2000, "The National Plan for Information Systems Protection Version 1.0" ("The National Plan for Information Systems Protection Version 1.0," January 2000,The White House).

This plan is often referred to by governments of other nations, when they formulate their own cyber security policy.

In this chapter, we will look at how this plan was developed in the first section 4.4.1, and then outline the plan in section 4.4.2.

Table 2: Recent changes in the U.S. critical infrastructure protection policy

Month / Year	Description
7 / 1996	Then- President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP).
10 / 1997	PCCIP released a report.
5 / 1998	Then- President Clinton signed the Presidential Decision Directive (PDD) 63.
1 / 2000	The National Plan for Information Systems Protection Version 1.0 was announced.

4.4.1 How the National Plan for Information Systems Protection Version 1.0 was developed

In response to the result of the Eligible Receiver exercise, an intrusion detection device was installed on every DOD network in addition to 24-hour monitoring. Other government agencies also began to take cyber security measures.

On the other hand, the industry was not paying as much attention as the government to their critical infrastructure protection.

Therefore, the government, which had been leaving the private sector to take care of their own key infrastructure protection and provision of stable service, changed their attitude and decided to collaborate with them to protect critical infrastructure according to the series of policies shown in Table 2.

(1) Recommendations by PCCIP

July 1996, then-President Clinton signed Executive Order 13010 to initiate:

— Establishment of the President's Commission on Critical Infrastructure Protection (PCCIP)

— Definition of critical infrastructure by the above organization

— Discussion on protective measures for the above critical infrastructure

PCCIP designated the following systems, which are crucial to national security and people's lives, as critical infrastructure:

— Power supply systems

— Gas/oil production systems

— Financial systems

— Transportation systems
— Water supply systems
— Emergency care service systems
— Public administration service systems

After studying protective measures for these systems, PCCIP issued the following recommendations in October 1997.

— Develop a wide range of programs to enhance cyber security awareness in the private sector.
— Facilitate collaboration and information sharing between the government and the private sector.
— Review the current legislation to eliminate elements that may hinder critical infrastructure protection.
— Promote research and development programs to develop technologies applicable to critical infrastructure protection.
— Expand national-level efforts to effectively make important resolutions and recommendations concerning critical infrastructure protection.

Table 3: The structure to implement PDD 63

Structure	Person or organization in charge	Responsibility
Assigning a National Coordinator	The First National Coordinator was Clarke (the current chair of the National Commission onTerrorism)	— Assist the President in implementation of PDD 63, and in charge of critical infrastructure protection as well as with domestic and foreign terrorism.
Establishing the National nfrastructure Protection Center (NIPC)	— Established within the FBI as a body to fuse together representatives from DOD, USSS (U.S. Secret Service), DOE (Dept. of Energy), DOT (Dept. of Transportation), the intelligence community, and so on, to promote collaboration among agencies and the private sector that are dealing with computer crimes and infrastructure protection. — Linked via networks with the federal government's monitoring center, private information centers and other facilities dedicated to countering cyber attacks.	— Provide warnings, analyses, and countermeasures in response to cyber threats, coordinate the effort of concerned organizations, mitigate attacks, and support recovery in the case of damage.
Establishing Information Sharing and Analysis Centers (ISACs)	— Established in each critical infrastructure industry. — The first ISAC, which was founded by the financial industry, started operation in October 1999.	— Report and exchange information about; (1) threats and damage from cyber attacks and computer crimes, (2) countermeasures and best practices, and (3) system vulnerabilities.
Establishing the National Infrastructure Assurance Council (NIAC)	— The chairperson is designated by the President. — The national coordinator serves as the executive director of the NIAC. — The members of the NIAC are appointed by the President, based on the recommendations of the major agencies and the National Economic Council (NEC), from private sector entities representing the critical infrastructure and from local governments.	— Meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructure.
Establishing the Critical Infrastructure Assurance Office	— Organized within the Department of Commerce.	— Provide support to the national coordinator's work in developing a national plan for protecting critical infrastructure. — Integrate the security measures developed by critical infrastructure industries into the national plan. — Analyze the federal government's dependence on critical infrastructure. — Help coordinate national education and awareness programs for cyber security, and legislative affairs.

Source: PDD 63, May 22, 1998, The White House

This was the first time that the government mentioned the private sector activities related to critical infrastructure protection.

(2) Presidential Decision Directive 63

In response to the recommendations by PCCIP, then- President Clinton, following additional discussions in NSC, signed Presidential Decision Directive (PDD) 63 in May 1998. The Directive prescribes:

— To build a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increase security of government systems by the year 2000.

— To immediately establish a national center to warn of and respond to cyber attacks.

— To address the cyber and physical infrastructure vulnerabilities of the federal government by requiring each department and agency to work to reduce its exposure to new threats.

— To require the federal government to serve as a model to the rest of the country, including state governments and enterprises, on how infrastructure protection is to be attained.

— To seek the voluntary participation of private industries to meet common goals for protecting our critical systems through public-private partnerships.

— To protect privacy rights and not to hinder free competition in the market while implementing cyber security policies.

— To seek full participation and input from Congress, in terms of overall cyber security protection.

In addition, PDD 63 orders the setting up of a structure as shown in Table 3 to deal with the challenge.

To implement PDD 63, the following National Plan for Information Systems Protection Version 1.0 was developed.

4.4.2 Outline of the National Plan for Information Systems Protection Version 1.0

Based on PDD 63, then- President Clinton set the National Plan for Information Systems Protection Version 1.0 in January 2000.

(1) Goals of the National Plan Ver. 1.0

The goals set up for the National Plan Ver. 1.0 are as shown in Table 4.

(2) Programs for the National Plan Ver. 1.0

To achieve the above goals, the programs shown in Table 5 were developed for the National Plan Ver. 1.0.

(3) Government organizations to carry out the National Plan Ver. 1.0

Figure 1 shows the government organizations that will carry out the National Plan Ver. 1.0. As indicated, the government is addressing critical infrastructure protection from a variety of viewpoints, including national security, R&D, standardization of technology and methods, human resource development, and information provision and analysis.

(4) Toward Version 2.0

As explained above, the National Plan Ver. 1.0 focuses on critical infrastructure protection activities initiated by the federal government. The version number is added because the Plan, which is now in the initial phase, is supposed to evolve in the future. The focus of attention toward the following phase is how private, public and local organizations are involved and expected to play

Table 4: Goals of the National Plan Ver. 1.0

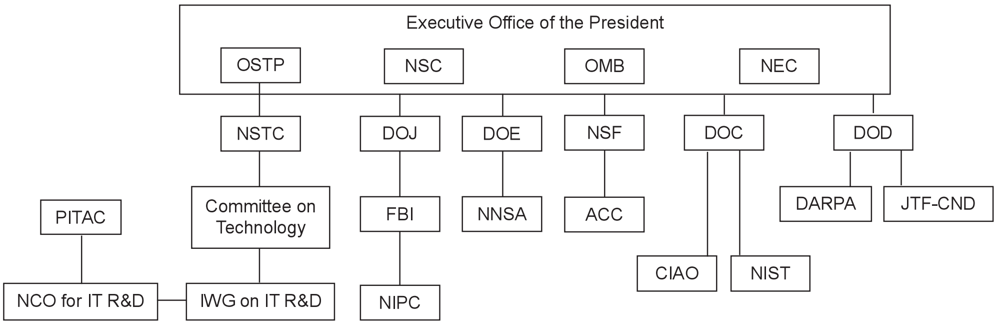
Category	Outline
Prepare and Prevent	— Minimize damage in case of a cyber attack on critical infrastructure. — Allow the attacked infrastructure to keep functioning without suspension of service.
Detect and respond	— Timely isolate, analyze, and confine cyber strikes, so that the affected system can be quickly restored and reconstructed.
Build strong foundations	— Develop a structure, human resources, and legislation, so that national-level prevention and detection of cyber attacks on critical infrastructure are provided.

Table 5: Programs to achieve the goals of the National Plan Ver. 1.0

Category	Program#	Outline
Prepare and prevent	1	Identify critical infrastructure assets and shared interdependencies and address vulnerabilities
Detect and respond	2	Detect attacks and unauthorized intrusions
	3	Develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law
	4	Share attack warnings and information in a timely manner
	5	Create capabilities for response, reconstitution, and recovery
Build strong foundations	6	Enhance research and development in support of Programs 1 - 5
	7	Train and employ adequate numbers of information security specialists
	8	Outreach to make Americans aware of the need for improved cyber-security
	9	Adopt legislation and appropriations in support of Programs 1 - 8
	10	In every step and component of the plan, ensure the full protection of American citizens' civil liberties, their rights to privacy, and their rights to the protection of proprietary data

Source: The National Plan for Information Systems Protection Version 1.0, January 2000, The White House

Figure 1: Organizations related to critical infrastructure protection policies in the U.S.



Organization names

OSTP: Office of Science and Technology Policy

NSTC: National Science and Technology Council

IWG: Interagency Working Group,

PITAC: President's Information Technology Advisory Committee

NCO: National Coordination Office

NSC: National Security Council

OMB: Office of Management and Budget

NEC: National Economic Council

DOJ: Department of Justice,

FBI: Federal Bureau of Investigation

NIPC: National Infrastructure Protection Center

DOE: Department of Energy

NNSA: National Nuclear Security Administration

NSF: National Science Foundation

ACC: Advisory Committee for Cyberinfrastructure,

DOC: Department of Commerce

CIAO: Critical Infrastructure Assurance Office

NIST: National Institute of Standards and Technology

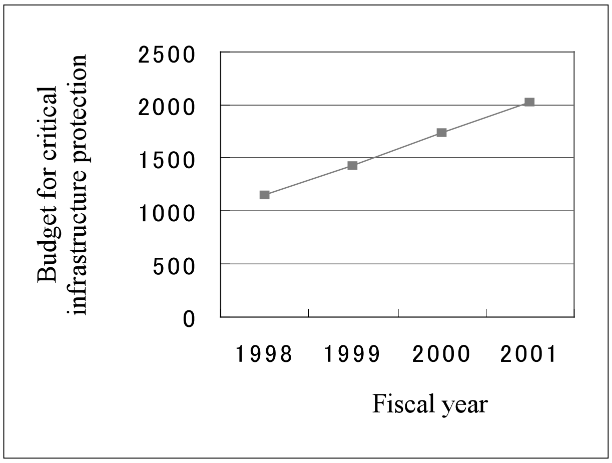
DOD: Department of Defense

DARPA: Defense Advanced Research Projects Agency

JTF-CND: Joint Task Force on Computer Network Defense certain roles independently or in collaboration with the government in order to protect their own critical infrastructure. The Bush administration is now working on the next version of the National Plan, which is being developed based on the previous version by integrating a wide range of opinions from Congress, state governments, industries, and local communities as well as from the public at large.The National Plan Version 2.0 will be released this fall.

4.5 The U.S. Government Budget to Protect Critical Infrastructure

Figure 2: U.S. government budgetary trends (critical infrastructure protection)



Source: Budget of the United States Government, Fiscal

Figure 2 shows the trend in the U.S. government budge to protect critical infrastructure.

Figure 2 indicates that the U.S. government budget to protect critical infrastructure has been on a steady rise.

4.6 Cyber Protection after the September 11 Attacks

On October 9, President Bush assigned Richard Clarke, who is the current chairman of the National Commission on Terrorism, as the special advisor to the President on Cyberspace Security. His mission was; i) immediately create a highly secured information system, and ii) establish a system that minimizes damage caused in case of cyber attacks ("Fact Sheet on New Counter-Terrorism and CyberSpace Positions," October 9, 2001,The White House).

Immediately after the assignment, Special Advisor Clarke announced a plan to develop GOVNET, a network dedicated to government organizations ("Top Cybercop Wants New Net," October 10, 2001,Associated Press).

The House Committee of Science held a public hearing on cyber security protection on October 10 ("Committee hears sobering news on nation's cyber security," October 10, 2001, Committee on Science, US House), where lawmakers, who were seriously concerned about the threat of cyber strikes, and invited experts actively discussed what the U.S. government was expected to do in the short, medium and long ranges.

Following this, Associate Press reported on October 11 that the federal government was planning a cellular system that would allow priority communications by emergency crews and government officials during a crisis. According to the report, the government was going to secure priority circuits for 500 users in the following two months and for 50,000 users by the end of 2002 (U.S. Plans New Cellular System," October 11, 2001,Associated Press).

On October 16, President Bush signed an executive order on critical infrastructure protection from cyber attacks that demands; i) continuous protection of critical infrastructure, ii) development of emergency communication networks, and iii) establishment of the President's Critical Infrastructure Protection Board.The Board is positioned as the highest-level authority to oversee planning and coordination of efforts to protect the private sector's critical infrastructure, public sector's information systems, and critical information systems for national security.

On the other hand, in Japan, the Cabinet decided to establish the Emergency Anti-Terrorism Headquarters, which on the same day, released emergency measures to combat terrorism. Among these measures, top priority items were identified on October 12, one of which was "enhancing the capability to counter cyber terrorism." More specifically, it was required to enhance the ability to counter cyber terrorism through reinforcing and expanding personnel involved, gathering information, increasing more sophisticated detection, analysis, and examination devices, strengthening protection of critical infrastructure, and so on.

Meanwhile, on October 10, the IT Strategy Headquarters convened the IT Security Promotion Committee to discuss and formulate a policy to deal with cyber terror attacks, which emphasized closer partnerships between the government and private sector.

4.7 Conclusion

This report provided an overview of the U.S. effort to develop cyber security policies from an early stage to address the increasing cyberspace threat.

Ahead of other countries in the world, the U.S. government has developed the National Plan for Information Systems Protection Version 1.0. While establishing a structure to carry out the plan, they are actively tackling measures in areas such as R&D, development of human resources, legislation, privacy protection, and governmental funding. In particular, their emphasis on protection of critical infrastructure owned by private and public sector entities, based on the awareness that malfunction of these systems can cause a nation-wide crisis, provides us with a lot of useful information.

Meanwhile, we should also be aware of the risk that our cyberspace vulnerabilities can cause damage not only to our country but also to other countries. Cyber attackers often make use of third-party computers to prevent backward tracing. If an attacker carries out a strike via a computer in Japan, the victim may take our country as the home of the criminal.

So far, even the U.S., the country most prepared for cyber strikes, does not seem to provide perfect critical infrastructure protection. Besides, as they often compare it to dog years, information technology is advancing so rapidly that a newly developed technology to enable higher security can soon become obsolete.

Therefore, it is important for us to immediately strengthen cyber security and to keep our countermeasures up to date.

From this point of view, we must have been quick enough when, in the wake of the terrorist attacks in the U.S., we started taking actions to combat cyber terrorism, lead by the Emergency Anti-Terrorism Headquarters and IT Strategy Headquarters.

The U.S. government is expected to announce the National Plan for Information Systems Protection Version 2.0, an upgrade from Version 1.0, in this fall. While making use of it as a helpful guide, the Japanese government should develop its own policy to protect the nation's information systems.

(Original Japanese version: published in October 2001)