National Cyber Security Masterplan

2011. 8. 2

National Cyber Security Masterplan(Summary)

▶ Protecting national cyber space from cyber attacks ◀

I Purpose

The Masterplan is a comprehensive response strategy at the national level in order to effectively deal with national cyber threats which are getting increasingly sophisticated and intelligent.

II Progress

11 May, 2011	The 'National Cyber Security Strategy Council' decided on the establishment of the Masterplan.
13 May~5 July, 2011	A draft was devised jointly by relevant organizations in consultation with experts
6 July~18 July, 2011	The Masterplan was deliberated and resolved at the 'National Cyber Security Countermeasure Council' meeting
2 August, 2011	50 deliverables were drawn and implemented

III Key points

5 action plans

1. Establishing joint response system of private, public and military sectors
2. Strengthening the security of critical infrastructure and enhancing secrets protection
3. Detecting and blocking cyber attacks at the national level
4. Establish deterrence through international cooperation
5. Building cyber security infrastructure

Organizing the response system and establishing roles within the government departments

- Establishing 「National cyber threat joint response team」 comprised of Private, Public and military sectors under the National Cyber security center(NCSC) in order to strengthen the cooperative ties such as cyber threat information sharing among participating organizations

  ※ 'Synthetic Judgement' · 'Joint monitoring' · 'Joint analysis' · 'Joint investigation' comprise 「The national cyber threat joint response team」 which started operating at full capacity in Jan. 2012.

- Establishing roles among relevant organizations such as the National Intelligence Service(NIS, overall control in times of peace and crisis), Korea Communications Commission(KCC, supervision over broadcasting and communications) and Ministry of Public Administration and Security(MOPAS, e-government service to the public, National Computing and Information Agency(NCIA) operating under MOPAS, and support for cyber security activities of local governments)

Major imperatives

1 Establishing cyber threat early detection and response system

- Setting up 「3-tier defence system」 connecting international gateway, ISPs and end-users(organizations and consumers) in order to detect and block cyber attacks in advance
- Strengthening response system in financial sector by reinforcing security systems in financial institutions and expanding security monitoring services to insurance companies and credit card corporations
- Reinforcing cyber restoration system by developing and distributing anti-virus softwares for the exclusive use of Zombie PCs to help rapid recovery and enhancing cooperative relations between the private and the public sectors; expanding the size and number of DDoS Cyber Urgent Shelters

2 Improving the level of security for critical information and facilities

- Expanding secret management system and upgrading encryption system to protectational confidential information
- Strengthening security measures for information and communications system in critical infrastructures such as electric power stations and transportation facilities; establishing immediate checking system comprising related organizations
- Tightening up security measures and defining clear responsibilities when outsourcing; making it mandatory to establish a system that diagnoses vulnerabilities of government S/W security

3 Developing platform that would enable a stronger cyber security

- Strengthening legal framework dealing with cyber threats by amending 'National Cyber Security Management Regulation' and promoting enactment of new related laws
- Establishing sector-specific circulation systems designed to create arms exclusively for cyber security, reinforce manpower and train technical professionals
- Providing support for exporting Information Protection Products and increasing the budget for information protection R&D (5→10%)

4 Establishing deterrence against cyber provocation and strengthening international cooperation

- Expanding bilateral or multilateral cooperative relations in cyber security area and establishing information sharing systems with other leading countries and international organizations
- Operating 「private verification scheme」 in order to deal with the public suspicion over a perpetrator and their motivation, and build public confidence

- Fostering and improving joint training between related organizations to help them increase their ability to effectively respond to cyber crisis

5 Elevating the level of security management of critical information and facilities

- Establishing 「Information Protection Day」(legal anniversary) at the national level in order to raise public awareness and expanding the base in cyber security area

  ※ Wednesday of the second week of July is proclaimed to be 'National Information Protection Day'; and the month of July 'the Month of Information Security'. Joint government ceremony was held to celebrate the first 「National Information Portection Day」 on 11 July, 2012.

- Promoting 「Clean Internet Campaign」 in the private sector to protect personal information and to prevent personal computers from turning into Zombie PCs,; strengthening the cyber security education in elementary, middle and high schools budget for information protection R&D (5→10%)

National Cyber Security
Master Plan

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu