The Coverage and Policies of Critical Infrastructure Protection in U.S.

Regarding the issue of critical infrastructure protection, the emphasis in the past was put on strategic facilities related to the national economy and social security merely based on the concept of national defense and security1. However, since 911 tragedy in New York, terrorist attacks in Madrid in 2004 and several other martial impacts in London in 2005, critical infrastructure protection has become an important issue in the security policy for every nation. With the broad definition, not only confined to national strategies against immediate dangers or to execution of criminal prevention procedure, the concept of "critical infrastructure" should also include facilities that are able to invalidate or incapacitate the progress of information & communication technology. In other words, it is elevated to strengthen measures of security prevention instead. Accordingly, countries around the world have gradually cultivated a notion that critical infrastructure protection is different from prevention against natural calamities and from disaster relief, and includes critical information infrastructure (CII) maintained so that should be implemented by means of information & communication technology into the norm.

In what follows, the International CIIP Handbook 2008/2009 is used as a research basis. The Subjects, including the coverage of CIIP, relevant policies promoted in America, are explored in order to provide our nation with some references to strengthen the security development of digital age.

1. Coverage of Important Critical Information Infrastructures

Critical infrastructure is mainly defined in "Uniting and Strengthening our country by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, as known as Patriot Act of the U.S., in section 1016(e)2 . The term ‘critical infrastructure’ refers to "systems and assets, whether physical or virtual, so vital to our country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." In December 2003, the Department of Homeland Security (DHS) promulgated Homeland Security Presidential Directive 7 (HSPD-7)3 to identify 17 Critical Infrastructures and key resources (CI/KR) ,and bleuprinted the responsibility as well as the role for each of CI/KR in the protection task. In this directive, DHS also emphasized that the coverage of CI/KR would depend on the real situations to add or delete sectors to ensure the comprehensiveness of critical infrastructure. In March 2008, DHS added Critical Manufacturing which becomes the 18th critical infrastructure correspondent with 17 other critical infrastructures. The critical infrastructures identified by DHS are: information technology, communications, chemical, commercial facilities, dams, nuclear reactors, materials and waste, government facilities, transportation systems, emergency services, postal and shipping, agriculture and food, healthcare and public health, water, energy (including natural gas, petroleum, and electricity), banking and finance, national monuments and icons, defense industrial Base, and critical manufacturing.

2. Relevant Policies Previously Promoted

With Critical Infrastructure Working Group (CIWG) as a basis, the President's Commission on Critical Infrastructure Protection (PCCIP) directly subordinate to the President was established in 1996. It consists of relevant governmental organizations and representatives from private sectors. It is responsible for promoting and drawing up national policies indicating an important critical infrastructure, including natural disasters, negligence and lapses caused by humans, hacker invasion, industrial espionage, criminal organizations, terror campaign, and information & communication war and so on. Although PCCIP no longer exists and its functions were also redefined by HDSP-7, the success of improving cooperation and communication between public and private sectors was viewed as a significant step in the subsequent issues on information security of critical infrastructure of public and private sectors in America. In May 1998, Bill Clinton, the former President of the U.S., amended PCCIP and announced Presidential Decision Directive 62, 63 (PDD-62, PDD-63). Based on these directives, relevant teams were established within the federal government to develop and push the critical infrastructure plans to protect the operations of the government, assist communications between the government and the private sectors, and further develop the plans to secure national critical infrastructure.

In addition, concrete policies and plans regarding information security of critical infrastructure would contain the Defence of America's Cyberspace -- National Plan for Information Systems Protection given by President Clinton in January, 2000 based on the issue of critical infrastructure security on the Internet which strengthens the sharing mechanism of internet information security messages between the government and private organizations. After 911, President Bush issued Executive Order 13228 (EO 13228) and Executive Order 13231 to set up organizations to deal with matters regarding critical infrastructure protection. According to EO 13228, the Office of Homeland Security and the Homeland Security Council were established. The duty of the former is mainly assist the U.S. President to integrate all kinds of enforcements related to the protection of the nation and critical infrastructure so as to avoid terrorist attacks, while the latter provides the President with advice on protection of homeland security and assists to solve relevant problems. According to EO 13228, the President's Critical Infrastructure Protection Board directly subordinate to the President was established to be responsible for offering advice on polices regarding information security protection of critical infrastructure and on cooperation plans. In addition, National Infrastructure Advisory Council (NIAC), which consists of owners and managers of national critical infrastructure, was also set up to help promote the cooperation between public and private sectors. Ever since the aforementioned executive order, critical infrastructure protection has been more concrete and specific in definition; for instance, to define critical infrastructure and its coverage through HSPD-7, the National Strategy for Homeland Security issued in 2002, the polices regarding the National Strategy to Secure Cyberspace and the National Strategy for Physical Protection of

Critical Infrastructure and Key Assets addressed by the White House in 2003; all of this are based on the National Strategy for Homeland Security. Moreover, the density of critical infrastructure protection which contains virtual internet information security was enhanced for the protection of physical equipment and the protection from destruction caused by humans.
Finally, judging from the National Infrastructure Protection Plan (NIPP), Sector-Specific Plans (SPP) supplementing NIPP and offering a detailed list of risk management framework, along with National Strategy for Information-Sharing, the public-private partnership (PPP) and the establishment of information sharing mechanism are highly estimated to ensure that the network of information security protection of critical infrastructure can be delicately interwoven together because plenty of important critical infrastructures in the U.S. still depend on the maintenance and operation of private sectors.

1.Cf. Luiijf, Eric A. M. , Helen H. Burger, and Marieke H. A. Klaver, “Critical Infrastructure Protection in the Netherlands：A Quick-scan”. In：Gattiker, Urs E. , Pia Pedersen, amd Karsten Petersen (eds.) . EICAR Conference Best Paper Proceedings 2003, http://cip.gmu.edu/archive/2_NetherlandsCIdefpaper_2003.pdf （last accessed at 20. 07. 2009）
2.For each chapter of relevant legal cases, please visit http://academic.udayton.edu/health/syllabi/Bioterrorism/5DiseaseReport/USAPatriotAct.htm. The text regarding the definition of critical infrastructure is cited as "Critical Infrastructure Defined- In this section, the term “critical infrastructure” means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matter. "
1.Cf. Luiijf, Eric A. M. , Helen H. Burger, and Marieke H. A. Klaver, “Critical Infrastructure Protection in the Netherlands：A Quick-scan”. In：Gattiker, Urs E. , Pia Pedersen, amd Karsten Petersen (eds.) . EICAR Conference Best Paper Proceedings 2003, http://cip.gmu.edu/archive/2_NetherlandsCIdefpaper_2003.pdf （last accessed at 20. 07. 2009）
2.For each chapter of relevant legal cases, please visit http://academic.udayton.edu/health/syllabi/Bioterrorism/5DiseaseReport/USAPatriotAct.htm. The text regarding the definition of critical infrastructure is cited as "Critical Infrastructure Defined- In this section, the term “critical infrastructure” means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matter. "
3.Introduction of Consumer Protection in Taiwan , Republic of China , Consumer Protection Commission (CPC), Executive Yuan.http://www.fas.org/irp/offdocs/nspd/hspd-7.html (Last visit 2008/6/27)

Release： 2013/04