Introduction to Critical Infrastructure Protection

The security facet of cyberspace along with a world filled with CPU-controlled household and everyday items can be examined from various angles. The concept of security also varies in accordance with different stages of national conditions and industrial development in different nations. As far as our nation is concerned, the definition of security industry is "an industry offering protection for human bodies, important infrastructure, information, financial system, as well as offering equipment to defend the security of national lands and the service"1 as initially defined by "Security Industry Program Office." Judging from the illustration of the definition, the security industry should be inter-disciplinary and integrative, which covers almost all walks of life and fields, such as high-tech industrial security management, traffic & transportation security management, fire control and prevention against natural calamities, disaster relief, information security management, security management in defense of national borders, and prevention of epidemics.

After the staged mission, "e-Taiwan program", was accomplished in 2007, our government hoped to construct a good surrounding by creating a comfortable life from a user's point-of-view. This was hoped to be achieved by using "the development of a high-quality internet society" as a main source by using innovative services, internet convergence, perceptive environment, security, trust, and human machine linkage. At the Economic Development Vision for 2015: First-Stage Three-Year Sprint Program (2007~2009) formulated by the Executive Yuan, wireless broadband, CPU computer-controlled items all have become part of our every day lives, and healthcare, along with the green industry are listed as the next emerging industries; whereby the development of relevant critical technologies is hoped to be promoted to create higher industrial values and commercial opportunities. However, from a digitally-controlled-life viewpoint, the issue concerned by all walks of life is no longer confined to the convenience and security of personal life but gradually turns to protection of security of a critical infrastructure (CI) run by using information technology. For instance, finance management, stock market, communication network, harbors and airports, high speed rail, R&D of important technology, science parks, water purification facilities, water supply facilities, power, and energy facilities. 2Because security involves resources related with people's most fundamental living needs and is the most elementary economic activity of the society, it is regarded as an important core objective to promote the modern social security system. Therefore, critical infrastructure protection requires more dependence on information and communication technology to maintain the stability of finance and communication, as well as the security of facilities related with supply and economy of all sorts of livelihoods in order to ensure regular operation.

With the influence of information and communication technology on the application of critical infrastructure on the increase, the society has increasingly deepened its dependence on the security of our cyber world. The concept and connotation of information security also keep extending with it toward the aforementioned critical infrastructure protection planning, making critical information infrastructure protection (CIIP) and critical infrastructure protection (CIP) more inseparable in concept3 , and becomes an important goal of policy implementation to achieve the vision of a digital lifestyle which is secure for every nation. In recent years, considerable resources have been invested to complete an environment whereby a legal system of "smart lifestyle" is developed. However, what has been done for infrastructure protection continues to appear as not being comprehensive enough. This includes vague definitions, scattered regulations and policies, different protection measures taken by different authorities in charge, obvious differences in relevant risk management measures and in the magnitude of management planning of information security and so on. These problems all influence the formation of national policies and are the obstacles to the promotion of relevant industrial development. In view of this, the 2008/2009 International CIIP Handbook will be used as the cornerstone of research in this project. After the discussion on how critical infrastructure protection is done in America, Germany and Japan, the contents of norms of regulations and policies regarding critical infrastructure protection in our nation will be explored to make an in-depth analysis on the advantages and disadvantages of relevant norms. It is hoped to find out what is missing or omitted in the regulations and policies of our nation and to make relevant amendments. Suggestions will also be proposed so that the construction of a safe environment whereby the digital age of our nation can be expanded to assist the "smart lifestyle" to be developed further.

1.See http://tsii.org.tw/modules/tinyd0/index.php?id=14 (last visited May 24, 2009)

2.For "2008 International Conference on Homeland Security and Application of Technology in Taiwan ~ Critical Infrastructure Protection~", please visit http://www.tier.org.tw/cooperation/20081210.asp (last visit date: 05/17/2009).

3.For critical infrastructure protection, every nation has not only proceeded planning for physical facilities but put even more emphasis on protection jobs of critical information & communication infrastructure maintained via the information & communication technology. In the usage of relevant technical terms, the term "critical infrastructure" has also gradually been used to include the term "critical information & communication infrastructure". Elgin M. Brunner, Manuel Suter, Andreas Wenger, Victor Mauer, Myriam Dunn Cavelty, International CIIP Handbook 2008/2009, Center for Security Studies, ETH Zurich, 2008. 09, p. 37.

Release : 2013/04

Tag