Cybercrime strong foundation for blocking cyber attacks.

Design, Fashion

Cybercrime goes beyond the technical, transnational dimension and involves offenders who deliberately fashion their attacks to exploit the potential weaknesses present in the infrastructure’s transnational nature. It threatens the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carries messages, and process information. Cybercrime is one of the fastest growing non-violent crimes in the Asian region. It takes a great deal of technical expertise and co-operation, both local and foreign, in order to address such problems. This crime affects different countries in varying degrees, depending on the extent of the legislative enactment of each country. Like in the Philippines, each of its government systems is being affected by these cyber attacks. Developing a National Cyber Security will build a strong foundation for blocking Cyber attacks.

Based on the study of (Sucahyo and Hasibuan, 2012), Indonesia as a country that is growing rapidly in the ICT sector has made efforts to address cyber threats. (Sucahyo and Hasibuan, 2012) describes the state of the art national cybersecurity in Indonesia, which is consist of five aspects, such as Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. This paper also proposed national cybersecurity principles and strategies for implementation and development national cybersecurity in Indonesia. However, in the Philippines, several problems relying on cyberterrorism attacks have been reported since its own cybersecurity systems aren’t yet compatible to combat such cyber threats (Domingo, 2016). On the other hand, Cyber-

warfare is no longer science fiction and the debate among policy-makers on what norms will guide behavior in cyber-space is in full swing (Maurer, 2011).

In 2010, (Maurer, 2011) the U. S. reversed its long-standing policy position by co-sponsoring for the first time a draft resolution on cyber-security that has been introduced in the UN General Assembly by the Russian Federation since 1998.

Generally, two principal streams of negotiations regarding cyber-security can be distinguished at the United Nations: a politico-military stream focusing on cyber-warfare (Maurer, 2011) and an economic stream focusing on cyber-crime. Moreover, Cybersecurity has become a matter of national, economic, and societal importance (Maurer, 2011). Present day attacks on the nation's computer systems (Domingo, 2016) do not simply damage an isolated machine or disrupt a single enterprise system. Instead, modern attacks target infrastructure that is integral to the economy, national defense, and daily life (Walker, 2015). Computer networks have joined food, water, transportation, (Walker, 2015) and energy as critical resources for the functioning of the national economy. (Domingo, 2016) stated that when one of these key cyberinfrastructure systems is attacked, the same consequences exist for a natural disaster or terrorist attack. National or local resources must be deployed. Decisions are made to determine where to deploy resources.

According to (Schneier et al., 2014), the study on the context of cyber terrorism is quite complex as it is about threat perception which makes the

concept different from one to another. Understanding similarities and (Maurer, 2011) differences in perception of what constitutes cyberterrorism can provide insight on the concept of cyberterrorism (Schneier et al., 2014). Finally, the threat for the countries will come from cyber threats (Sucahyo and Hasibuan).

Cyber threats potentially attack national assets and interests (Walker, 2015). Furthermore, every country needs to develop national cybersecurity strategies to anticipate the cyber threats (Domingo, 2016). National or local resources must be deployed (Maurer, 2011). Decisions are made to determine where to deploy resources (Schneier et al., 2014).