TALKING POINTS

Asan Plenum 2015: “Is the U.S. Back?”
www.asanplenum.org

RELEASE EMBARGO DATE: April 28, 2015 at 9:00 AM

Panel: Cyberwar
Date/Time: Tueseday, April 28, 2015 / 15:30-16:45
Talking Points for: Park Nohyoung, Korea University

The session description correctly describes what has happened in and through cyberspace, including the notorious case of North Korea's hacking against Sony Pictures last year. However, as President Obama correctly confirmed, what North Korea did is not "an act of war". Instead, he called it "cyber vandalism". Cyberwar is often mentioned nowadays, and it is worrying many including the media. But cyberwar as such is not the proper terminology, and the attachment of the word "war" makes people think in the wrong way. Unfortunately, the term cyberwar has become a buzzword, being used by authorities and the media to describe any large-scale hacking intrusion. The term cyberwar should be used and understood strictly in respect to war or the use of force and armed attack in international law.

As the session description suggests, cyber attacks may be taking place in a largely unregulated environment. Fortunately, there is internationally a significant effort being made for regulating cyberspace or the use of information and communication technologies (ICTs). For example, there is the Cyber Crime Convention mainly comprised of members of the Council of Europe. Cyberwar or cyberwarfare, more correctly, has also been frequently discussed internationally, especially since Estonia was "attacked" in 2007. For example, the UN Group of Governmental Experts in information security, which was initiated by Russia some 15 years ago, has been working for an agreement over the application of international law on the use of ICTs by states. The United States and European countries under the NATO as well as the European Union have also announced their national cyber security strategies.

Most recently, there is growing consensus that existing international law does apply to cyberspace. Why? Cyberspace is the same as other traditional domains like land, sea, airspace and outer space, where individuals, companies and states operate for their objectives. In this respect, existing international law should and does apply to cyberspace. States exercise their sovereign rights over cyber infrastructures and related cyber activities or operations. Due to its own characteristics, however, additional international norms on cyberspace are agreed to develop over time.

What is the existing international law applicable to cyberwar or cyberwarfare? The existing international law governing cyberwarfare are *jus ad bellum*, which governs the resort to force by states as an instrument of their national policy, and *jus in bello*, which regulates the conduct of armed conflict.