ASAN PLENUM 2015

SESSION SKETCH

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

Panel: Cyberwar
Date/Time: Tuesday, April 28, 2015 / 15:30-16:45
Moderator: David Sanger, *The New York Times*
Speakers: Van Jackson, Center for a New American Security
Park Nohyoung, Korea University
Michael Raska, Nanyang Technological University
Ren Lin, Chinese Academy of Social Science

With recent events that exemplify the rise of cyberattacks against other nations and their infrastructures, session 2 entitled “Cyberwar” explored the implications of the changing nature of cyberspace. Led by moderator David Sanger, chief Washington correspondent for *The New York Times*, this panel juxtaposed cyber warfare with conventional warfare and examined the new challenges that arise from this new kind of security threat.

Mr. Sanger began by stating that a nation can conduct cyberwar without triggering an actual war. Because of the divide between the physical space and cyberspace, arms discussions are considered inappropriate when responding to cyberattacks. Thus, comparisons between nuclear attacks and cyberattacks are misleading. While the former are expensive and serve as a powerful deterrent, the latter are cheap and inexpensive to maintain as well as hard to attribute, which add to the tactical value of conducting them.

Mr. Sanger brought up the infamous North Korean Sony attacks to introduce his first question to the panelists. According to him, of all the different kinds of cyberattacks that have been conducted in the past, the 2014 Sony Pictures Entertainment hack was the most impactful. Intended to make a political point, North Korea’s cyberattack was in direct response to Sony’s planned release of the film “The Interview”, a comedy about a plot to assassinate North Korean leader Kim Jong-un. Given this, Mr. Sanger asked how North Korea conceptualizes cyberwar, especially in relation to its nuclear program.

The first speaker, Van Jackson, a Visiting Fellow of the Center for a New American Security, stated that North Korea does not treat cyberspace as a space that is distinctly military; it serves multiple purposes and goals. Consequently, this makes deterrence extremely difficult because of the many factors to consider when trying to understand the intentions behind North Korean cyberattacks. As such, the United States has attempted to categorize cyberattacks under the military realm in an effort to narrow and organize responses.

In this vein, Mr. Sanger asked for the speakers’ opinions on President Obama’s choice to label the Sony hack as cyber vandalism and not cyber war. According to Dr. Park Nohyoung of Korea University, Obama approached the issue in the appropriate manner. “War is a strong word”, he said in reference to its strong political and military connotations.

* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.

Speaker Michael Raska, Research Fellow in the Military Transformations Program at the S. Rajaratnam School of International Studies in Singapore, stated that cyber as an overall strategy has evolved over the past few years. Moreover, due to the progressive complexity and variant evolutions of technology depending on locality, every country has formed its own conception of cyber warfare. For example, China emulates Russia’s hybrid warfare, which integrates cyber tactics to supplement conventional warfare. In the United States, the Pentagon has officially recognized cyberspace as a new domain in warfare, adopting information warfare strategies known as weapons of mass effectiveness. Mr. Sanger pointed out that both Iran and North Korea have invested heavily in weapons of mass effectiveness. This alludes that both countries realize military arms are fundamentally not as effective and wide-ranged as cyber arms. While cyber weapons will never replace the potential devastation of military weapons, their limited strikes have great strategic effects. As follows, wired nations like the United States are often the most vulnerable to such strikes, while disconnected countries like North Korea are unaffected.

During the question and answer section of the panel, the discussion focused on finding the different thresholds for different responses to cyberattacks. A particularly interesting topic that came to light was if cyber war will ever kill. Dr. Jackson’s response was: “Cyber doesn’t kill; the *response* to cyber kills”. According to him, one should fear the threat of miscalculation, not of a “cyber Pearl Harbor”. One nation can misjudge and conduct a cyberattack that it believes is below a certain threshold only to suffer what can be perceived as disproportional retaliation leading to a dangerous escalation that will spill over into the physical realm. Moreover, because individual actors and not only governments can pose cyber threats, there is a growing need to codify rules of cyber warfare.

* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.