PacNet
Number 4A

Pacific Forum CSIS
Honolulu, Hawaii

Jan. 16, 2015

Cyber war, national security, and corporate responsibility
by Jongsoo Lee

Jongsoo Lee (jlee@brockcapital.com) is Senior Managing Director at Brock Securities LLC and Center Associate at Davis Center for Russian and Eurasian Studies, Harvard University.

The recent hacking of Sony Pictures, allegedly perpetrated by North Korea, and its aftermath may go down in history as the dawn of "cyber 9/11." This event raises important issues about the tension between free speech, national security, and corporate responsibility in the new era of cyber warfare.

What was disturbing about the way this incident unfolded was how Sony's provocation of North Korea with the planned release of a movie forced the US president to weigh in on a private company's business decisions and, in the process, metastasized into a potentially dangerous confrontation between the United States and an assertive nuclear power under an unpredictable tyrant.

In a free-market society, a company's right to pursue profit-generating business and exercise its freedom of speech is not in dispute. While some may object to a film featuring the assassination of the sitting head of state, Sony had the right to produce such a film. That does not necessarily mean that Sony's action was in the best interests of US national security. Although many in the US satirize Kim Jong Un, North Korea is a nuclear power with a significant and growing cyberattack capability. Pyongyang has been developing nuclear-tipped ICBMs and SLBMs that will one day reach the US mainland and, according to some analysts, already possesses the ability to launch an EMP attack that can paralyze the US national power grid.

In provoking Pyongyang, a fiercely nationalistic regime centered on the worship of the Kim dynasty that is paranoid about a US attempt to force a regime change, Sony risked inviting a North Korean reprisal without shoring up its own sloppy cyber security, which had made it the victim of past hacking attacks. In the resulting fallout, for which Sony was unprepared, the US as a nation was dragged into a potentially open-ended cyber war against Pyongyang when Obama vowed to retaliate. Unfortunately, by this time, the US as a nation had already suffered a setback, given the unprecedented damage done to a major US company, as well as the decision by Sony and the biggest US theatre chains to cancel the film's showings – a decision made without consulting the US government and which was seen as capitulation to foreign cyber terror and blackmail.

Would Sony or any other US film studio contemplate producing a movie featuring the CIA assassination of, say, Vladimir Putin, knowing that the Kremlin could annihilate the US with the push of a nuclear button and that Moscow has a potent cyber attack capability, especially now that Putin is under pressure from Western sanctions and an economic crisis? That movie too "has a right to be made" and might even be profitable, but it would likely enrage Putin and invite a reprisal, and rally public support for Putin by conjuring foreign conspiracies against a beleaguered Russia. None of these developments are in the US national interest.

None of this is to advocate government censorship and self-censorship. Rather, this is a call for a robust and reasoned national debate on the role of corporate responsibility in the new war on cyber terror. The key question is: how to keep cyber attacks elicited by and directed at private US entities from escalating into an all-out cyber or conventional war? Because it can be hard to identify the perpetrator of a cyber attack and certain entities are better shielded from cyber attacks, it is possible for a foreign entity or nation to inflict destruction on the US while escaping a punitive response. In this asymmetric cyber warfare, mutual deterrence can fail, which increases the incentive for cyber attacks, giving rise to an open-ended and uncontrollable escalation of cyber warfare.

The US as a nation is not well prepared for cyber war. US private entities and industries, including Hollywood and other parts of the media & entertainment industry, have a role to play in contributing to US national security. They can start by enhancing their own cyber security, while forging an effective strategic partnership with the US government in deterring and handling foreign cyber attacks. Such a partnership requires better coordination of cyber defenses and expanded sharing of actionable cyber threat intelligence between business and government, which must be part of a comprehensive national blueprint for cyber security. The US government, on its part, needs to work with foreign governments in adopting an international code of cyber conduct so as to prevent escalation of cyber warfare. Finally, they can also begin by appreciating that with freedom comes responsibility and that while everything may be fit for expression, freedom of speech and business operation in the cyber age beget a new dimension of security concerns.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed.