**APrIGF Delhi 2014**

**Workshop Summary Report**

**Date: August 4, 2014**

**Time: 3:30 PM**

**Workshop Title:** Cybersecurity policy, strategy and implementation in the Asia Pacific region: The nature of the heterogeneity and its implications

**Reported by & Contact Email:** Nir Kshetri (nbkshetr@uncg.edu)

**Moderators:** Nir Kshetri, Professor, Bryan School of Business and Economics, The University of North Carolina at Greensboro

**Panelists:**

**Onsite:**

Dr. Lailani Alcantara, Associate Professor, Ritsumeikan Asia Pacific University, Japan

Mr. Hideyuki Fujii, Researcher, InfoCom Research, Japan

Mr. Aroop Menon, Senior Product Marketing Specialist, SolarWinds, India

Dr. Kamlesh Bajaj, CEO, Data Security Council of India, India

**Remote:**

Dr. Hong Xue, Professor, Institute for Internet Policy & Law (IIPL), Civil Society, China, Asia-Pacific Group (she could not complete here talk due to technical problems)

**A substantive summary and the main issues that were raised**

There were about 30 people in the audience and about a quarter of them were women.

Nir Kshetri started the session introducing the panelists and the topic of the workshop. He provided some statistics illustrating the seriousness of cybercrime, concerns related to cybersecurity and the vicious circle of hype surrounding this issue. The most often cited figure for the annual worldwide loss to cybercrime is US$1 trillion and about 70% of the world's internet users have been victimized at some points in their lives by cybercriminals. Studies have found that consumers and businesses worry more about cybercrimes than about physical crimes. The panel discussed a number of high-profile policy initiatives being taken in some of the big Asian economies, mainly India, China, Japan and South Korea on the cyber-front. The panel also compared how the evolving cybersecurity frameworks in the Asia Pacific economies are similar to and different from the frameworks adopted by the EU and the U.S.

The panel took a look at the variation in power and influence of various stakeholder groups in the region. A comparison of China and India was provided for illustration. Trade associations such as National Association of Software and Services Companies (NASSCOM) are key players in India’s cybersecurity-related debate. As an example, the Data Security Council of India (DSCI), a self-regulatory member organization set up by NASSCOM, can impose a fine of up to US$1 million to member companies that fail to secure data. The Internet Society of China (ISC) can be considered as an entity that is most analogous to the NASSCOM. ISC, however, has been described as a "quasi-governmental" organization and hence mostly acts under the guidance of the government. Under China’s current institutional structures, trade associations and special interest groups are less prevalent and are not in a position to function in the way they do in the West or in India.

 The panel discussed a number of key issues facing the global cybersecurity landscape such as attribution problems, the situation of cyber-cold war and the complications associated with the creation and implementation of cyber-weapons such as Stuxnet. Note that Stuxnet worm was programmed to damage Iran's centrifuges at the Natanz nuclear site. It also emphasized the role of the private sector in enhancing cybersecurity with the illustration of the initiatives of India’s National Association of Software and Services Companies (NASSCOM) and the Data Security Council of India (DSCI). In India’s context, the panel discussed the constraints facing Indian government in strengthening cybersecurity and assessed the context of public-private partnership in this area.

### Also covered briefly in the panel was cyber-threats facing South Korea and current measures taken by the country such as the creation of cyber-command (2010), cyber-protection policy team at the Defense Ministry (2011), Cyber Policy Department (2013) and a plan to have a secretary of cybersecurity. It has also a team to engage in psychological warfare against North Korea. Mentioned in the panel are also South Korea’s cybersecurity-related cooperation with the U.S. and its intention to develop weapons similar to Stuxnet.

Also discussed in the panel was the evolving meaning of cybersecurity in Japan, various types of cyber-risks facing the country and recent initiatives taken by the Japanese government to address them. The panel provided a detailed review of Cybersecurity Strategy 2013 and analysis of some of the hot issues in the Japanese cybersecurity landscape such as Public-Private cooperation, Global cooperation and effects of 2020 Tokyo Olympic/Paralympic on the Japanese cybersecurity industry.

The panel also focused on cybersecurity from cultural and organizational perspectives. A key point was the importance of creating a culture of cybersecurity which requires changes in attitude and behavior in the cyberspace. The first step in this process is to create a sense of urgency by making people understand the threats to cybersecurity and the value lost due to cybercrimes.

**Conclusion & Further Comments:**

The rapidly evolving cybersecurity frameworks in major economies in the region have potential to significantly affect the regional and global cybersecurity landscapes. An issue raised in the question-answer session concerned about the session’s focus on only the big economies. This is a valid concern. It was agreed that more attention needs to be devoted to cybersecurity issues facing smaller and poorer economies in the region. At the same time, smaller economies in the region can learn from the bigger and more advanced economies in the region to develop cybersecurity-related frameworks, policies, and strategies.