Regional Collaboration in Cybersecurity

Presentation Summary

Robert D. Childs, Ph.D.

In his presentation, Dr. Childs argues for urgent and strengthened regional collaboration in cybersecurity. He opens with a 10-minute video of a possible scenario where former U.S. officials are playing the role of top government leaders who are gathered to discuss possible responses to an as yet unconfirmed cyberattack on U.S. critical infrastructure. Results of the emergency meeting will directly be briefed to the President. Dr. Childs believes that this simulation reveals the reality of cyberattacks and cyberwar, and nations must act in concert to find and implement appropriate responses. He provides a rundown of the strategic ramifications and issues of cyberattacks as follows:

- Estonia is one of the few countries to experience an open act of cyberterrorism and cyberwar; its experience is not an isolated one – it will be repeated in the future;
- the more advanced a country is in using technology, the greater the effects of a cyberattack or network denial of service will be;
- there is a need for a global perspective on how to deal with the effects of cyberisolation instigated by a determined enemy;
- the Internet is part of our lives now – we cannot simply disconnect from it, but we must determine how we are to live in it; cyber is virtual but has become the "fifth domain," (and the fourth commons) that is as real as any physical domain (land, sea, air and space); and
- the ability to assign attribution is key to dealing with the strategic impact of cyberattacks; with attribution, nations must build trust: trust in one another's desire for national security and trust to share information on cyberthreat warnings and indications; without trust, there can be no appropriate response or retaliation to a cyberevent.

Gross Domestic Product (GDP) leaders like the U.S. depend on the Internet to maintain positive GDP growth, but Dr. Childs cites that China and India have surpassed the rest of the world in numbers of Internet users with Vietnam coming up fast. The implication is that the ability to influence the governance of the Internet will be the countries with the most users, and it is thus incumbent upon all nations to seek collaboration to collectively improve cybersecurity.

Moreover, the techtronic forces driving global change on all aspects of human society are IT-based. Dr. Childs mentions two factors in particular: economic virtualization and margin expenses, and the technology itself. He points out that the explosion of online economic activity has gone hand-in-hand with the notion of borderless networks and now enhanced by cloud computing. Furthermore, economic virtualization has engendered technology expectations that are now "trickling up" from home use to work. Three technology-related trends will define change in the

future: the continued proliferation of commercial devices, the shift to Internal Protocol version 6 (IPv6) that will provide a massive increase in IP addresses from 2(32) to 2 (128), and the unabated growth and spread of social media and the "New Millenial" users. Dr. Childs notes that cloud computing will pose the next security challenge in four areas: trust (in turning over data to others), control (location of the servers), information assurance, and supply and demand.

Existing challenges continue to be daunting. Operationalizing the definition of 'cybersecurity' is a major and global issue. In the U.S., competing frames of what cybersecurity is revolves around four areas: economic prosperity, privacy rights and civil liberties, public safety and law enforcement, and national security.

Finally, he points out that if regional collaboration in cybersecurity is going to improve, nations have to address some key issues, namely information sharing, attribution and mitigation steps, rules of engagement, and the borderless nature of cyberspace (this is an important consideration if potential partners collaborate to organize a cyberspace joint area of operations that allows collaboration in a timely fashion).