CyberPro

December 19, 2008

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE

NSCI: NATO recently stood-up the Cooperative Cyber Defence Centre of Excellence in Estonia (CCD COE). What key activities to improve international cyberspace operations are underway via this Center of Excellence?

CCD COE: Our primary client is NATO. Therefore, we mostly work within the NATO framework, providing insight, subject matter expertise and assistance on various facets of cyber defence: providing input to NATO Cyber Defence concept development, organizing training and exercises, researching cyber events and problems as well as cornering the legal issues.

NSCI: What countries are participating in the activities of the CCD DOE?

CCD COE: There are currently seven Sponsoring Nations: Estonia, Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain. In addition, US and Turkey have announced their intent to join in the near future. The CCD COE is open to all NATO nations and may cooperate with other nations.

NSCI: What key challenges does the CCD COE face?

CCD COE: The main challenges surrounding Cyber Defence include: lack of universally agreed definitions and legal framework, attribution of cyber attacks, deeply integrated military and civilian assets as well as low resources required to develop offensive cyber capabilities.

NSCI: It has been 18 months since the cyber attacks on Estonia brought cyberspace to center stage. Can you comment on international efforts in general since that time?

CCD COE: The Estonia 2007 and Georgia 2008 cyber attacks have elevated the issue into public awareness. However, little measurable progress, aside from potentially increased funding for various national defensive programs, has been made. The international law is still quite vague on cyber attacks.

NSCI: What big picture lessons learned should the world take away from the Estonia attacks?

CCD COE: We need a universally agreed standard (backed by legal measures) that defines the use of cyber attacks. This would allow us to better coordinate the investigations and defense against cyber attacks.

NSCI: What does the CCD COE view as the most urgent international cyber threat(s) over the next several years?

CCD COE: State sponsored cyber attacks against critical (civilian) infrastructure as part of a wider political/military campaign. This would require a conflict between two or more technologically advanced states.

NSCI: What are the CCD COE priorities for 2009 and 2010?

CCD COE: As 2009 will be the first full year for the Centre, then number one priority is to execute Centre's Programme of Work for 2009. Main events include the Cyber Warfare Conference, scheduled in June and Cyber Defence Legal Conference, scheduled in September.

NSCI: Is there anything else you would like to add?

CCD COE: CCD COE's homepage is its final stage to come on-line. Address is www.ccdcoe.org Please contact CCD COE PAO Mr. Madis Tüür (madis.tuur@mil.ee) for further queries.