CyberPro

December 2010

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: ENEKEN TIKK

NSCI's Lindsay Trimble recently had the opportunity to interview Eneken Tikk, head of the Legal and Policy Branch at NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). She holds a Magister Juris degree from the University of Tartu and is currently pursuing a doctorate degree. After working many years for both government and private sector enterprises, advising on information law, she joined the Cooperative Cyber Defence Centre of Excellence activation team, later becoming the head of the Centre's Legal Task Team. Tikk headed the Cyber Defence Legal Expert Team involved in drafting the Estonian Cyber Security Strategy. She is also a frequent lecturer on information technology and information law in Estonian universities and the author of an information law textbook. Her areas of research interest include information technology and cybersecurity law, as well as legal policy.

NSCI: NATO's Cooperative Cyber Defence Centre of Excellence was created one year after the 2007 cyber attacks against Estonia. How did Estonia recover from the attacks and position themselves as the host of this international center?

TIKK: Although the Centre was formally established in 2007, Estonia offered the project to NATO back in 2003. Therefore, the 2007 attacks and the international attention Estonia received with handling the incident just boosted an already ongoing initiative. Of course, the Estonian political ambitions in the cybersecurity area create a "natural" environment for hosting the Centre of Excellence.

NSCI: What is the main mission of the Cooperative Cyber Defence Centre?

TIKK: The Centre was established to enhance NATO's cyber defense capabilities. This is done through research, analysis, education and training, lessons learned and consultations. The Centre is not an operational unit like a Computer Emergency Readiness Team. Instead, it focuses on after-action and trend analysis, exercises, best practices and an interdisciplinary approach combining military, technical and legal and policy expertise.

NSCI: The cyber attacks against Estonia were some of the first of their kind. Along with now hosting this NATO center of excellence, what other progress has been made to improve cybersecurity in the country since then? Have neighboring countries joined the cyber defense effort?

TIKK: There are still somewhat differing views on how "unique" the Estonian attacks were. The bottom line is that looking at them from an Estonian perspective, they were severe enough to reconsider

national approaches to cybersecurity. Immediately after the attacks, Estonia revised its implementation package for the Cyber Crime Convention. In 2008, new cybersecurity strategy was adopted. Estonia was one of the four nations to initiate NATO's cyber defense policy and also raised the issue in the European Union. Over three years, the lessons learned in 2007 have improved the awareness in general, but have also resulted in a more practical and focused national approach to cybersecurity.

Latvia and Lithuania are also founding members of the CCD COE. Both nations have recently revised their national strategic approaches to cybersecurity. Also, both countries have recently witnessed politically-motivated cyber attacks – the "Robin Hood" case in Latvia and the Sickle and Hammer defacements in Lithuania in 2008.

NSCI: Because of the lack of definitive boundaries in cyberspace, the question of attribution has been a major topic of discussion. How important is international cooperation to solving the problem of attribution?

TIKK: Attribution is one of the key issues for cybersecurity. It is, however, important to note that it is a fact of life and therefore equally an issue from a technical and legal point of view. In case attribution will not be resolved technically for critical information resources, legal concepts might become necessary to create presumptions that make it possible to attribute general responsibility. Such concepts, if deemed necessary, will definitely require international debate.

NSCI: Many legal experts have said the lack of internationally-agreed on definitions of cyberwar and cyber terrorism is the major obstacle to official international agreements. What do you think it will take to develop international agreement on cyber attack and warfare definitions, thresholds and acceptable conduct?

TIKK: The statement about the lack of legal definitions seems to develop into a myth that is harder and harder to overcome. Legal thresholds are specified both for warfare and terrorism and, at least when it comes to "cyber armed attacks," the current issue is not that there is no definition but that there are no cases so far that would be serious enough to trigger a military response. Categorizing a cyber attack as warfare is a political decision that won't be difficult to make once an incident of such severity occurs. Also, legal framework is already in place to outline a response to such attacks.

Current cyber conflicts fall into a paradigm that is hardly regulated on an international level as it concerns national security. This is the domain where the threshold of "national security relevance" needs to be figured out and implemented on a national level. Once we start seeing military action and armed attack equivalents in cyberspace, it will not be so difficult to reach the necessary consensus on an international level. The cyber conflict paradigm has simply not reached that level.

NSCI: Do the same rules apply to cyber conflict as the rules of armed conflict?

TIKK: In case a cyber conflict is by its effects comparable to an armed attack, the rules of armed conflict would apply. Categorizing cyber incidents will be the discretion of the victim state, but the national

decision will have to comply with the minimum requirements agreed upon at the international level. So far, most cyber incidents are by their nature either criminal or threaten national security, which primarily invokes the applicability of criminal and national security legal framework. The legal regimes that will apply differ to an extent by nation.

NSCI: How do we ensure flexibility in our legislation to accommodate the speed at which cyber threats evolve?

TIKK: Law is a discipline that regulates behavior and has regard to the facts and circumstances of life. Therefore it is difficult to foresee legal developments preceding technological ones. At the same time, the more we witness cyber incidents of the same type (political context, targeting critical information infrastructure), the better the legal communities will be in interpreting and implementing existing laws to efficiently correspond to the needs of areas of expertise involved in cyber incident handling.

NSCI: Along with the ever-evolving nature of cyber threats and the question of attribution, what are other obstacles to resolving this new type of legal case?

TIKK: The main challenge I see is making best use of the comprehensive approach. As threats evolve, we aren't investigating and solving incidents within one legal area or domain. Because of this, the effective defense and recovery from cyber attacks will depend on how well we can assess and exploit the strengths of different institutions and countries in global cybersecurity. There are many overlaps, but there are still too many gaps between the focus areas of major international organizations. It is important to understand what different organizations have to offer and how it can be linked with the needs and strengths of others. In the legal field, this requires thinking outside the box of just one legal area; the solutions to cybersecurity derive from cyber law (telecommunications, e-commerce, privacy regulation), criminal law, and also national security law and the law of armed conflict. Only combining the elements of these four fields will give us a complete understanding of existing remedies and solutions.

NSCI: What do you think about the idea of creating an international court specifically to hear cyber attack cases? Would this be a successful solution?

TIKK: There are already international courts that can and do hear cyber attack cases. Examples include the European Court of Human Rights, European Court of Justice and the ICJ. Nations are not restricted in bringing their disputes about cyber incidents to these courts. Estonia, for example, could have brought to international court the Russian refusal to provide assistance with the investigations of the Bronze Soldier attacks. Again, we still have to learn how to make better use of the existing legal framework before striving for new regulations and instruments.

Thank you very much for your time.