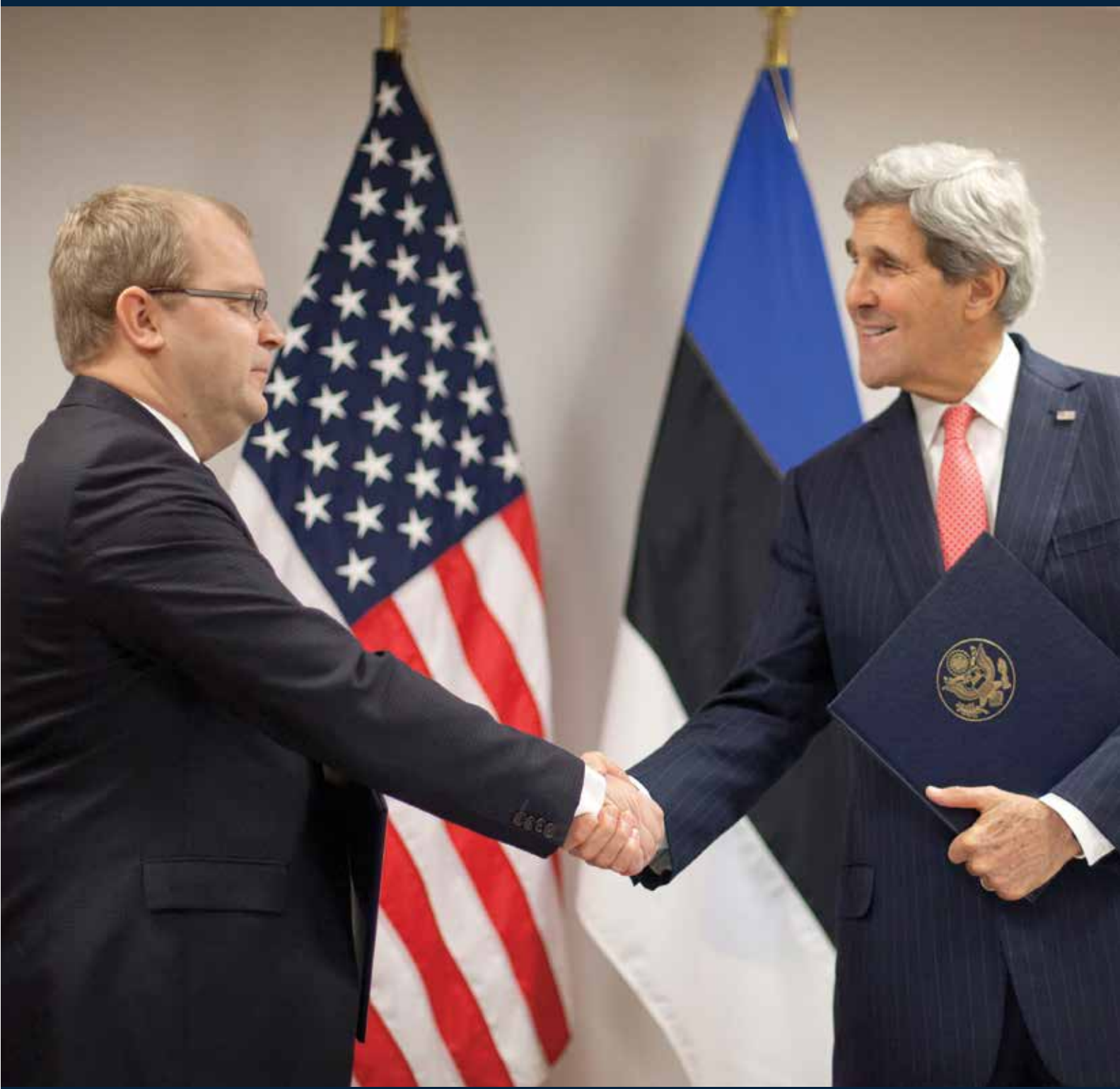
Striving for cyber excellence

Centre of Excellence leads NATO's efforts in cyber research and training

By Liis Vihul, NATO Cooperative Cyber Defence Centre of Excellence

In the midst of defense spending cuts, cyber security stands out as an exception to the prevailing cutbacks. States are boosting investments in this area, not only to improve their own resilience to hostile cyber operations, but also to develop offensive capabilities in support of their national and foreign security policy objectives. In light of the growing investment in and overall attention toward cyber security, the Tallinn, Estonia-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is attracting attention from NATO Allies to whom membership is open, and beyond.

Since the establishment of the first NATO Centre of Excellence (COE) in 2005, 18 COEs have mushroomed on the Euro-Atlantic map. Motivated by the prospect of a permanent NATO presence in their region, all seven Central and Eastern European states that acceded to NATO in 2004, including Estonia, already operate or are in the process of setting up a COE.[1] All COEs are idiosyncratic by virtue of the fact that they are designed to complement and enhance NATO capabilities in specific areas ranging from military medicine to energy security. Somewhat prophetically, Estonia saw its opportunity in cyber defense and presented NATO with a proposal to establish a cyber-oriented COE a few years before 2007, when the state became a victim of a large-scale cyber attack that thrust cyber security and defense to the forefront of political agendas.



Estonian Foreign Minister Urmas Paet, left, and U.S. Secretary of State John Kerry celebrate the signing of the U.S. Estonia Partnership Statement in December 2013. The document reaffirms the countries' commitment to a secure Internet. THE ASSOCIATED PRESS

CCDCOE: SIX YEARS LATER

Officially founded in 2008, the CCDCOE is currently a partnership of 11 states. In addition to Estonia's tricolor flag, the colors of Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain and the United States have been raised in the CCDCOE flag court. The Czech Republic, France and the United Kingdom will soon become member states, and Greece and Turkey are similarly undergoing the membership process. As such, and considering that COE membership is only open to NATO nations, the Tallinn COE unites many of the most prominent cyber states of the Alliance. Despite being ineligible for full membership, non-NATO nations may become contributing participants. Decisions are made on a case-by-case basis, and talks have already begun with Austria, Finland and Sweden.

Contrary to popular belief, the approximately 40-person CCDCOE is not an operational entity. Instead, it is oriented toward research and training and facilitating numerous academic, semi-academic and training events each year. Its work is divided into three categories: law and policy, technology and strategy. The center has a number of success stories that have earned it international visibility and credibility. These include the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, the inception of an annual conference tradition with high-level speakers and worldwide participants, and the ability to convene nearly 300 information security professionals annually for the live-fire cyber defense exercise dubbed Locked Shields.

THE TALLINN MANUAL

The question of how international law governs hostile cyber operations was embraced by numerous scholars as a direct result of the 2007 cyber attacks on Estonia and those against Georgia during its armed conflict with Russia the next year. The threat of highly disruptive cyber operations had evolved from a hypothetical scenario to a real world phenomenon. The unique characteristics of cyberspace and operations in this environment raise new and difficult issues for legal scholars. These issues include the speed with which events can unfold and consequences can manifest themselves, and the engagement of states not directly involved as originators and targets (either as simple transit states or those whose territory is used, knowingly or not, to carry out the operations, for example, by setting up a command and control server for a botnet attack). Other issues include the difficulties of determining the originators of attacks, the intangibility of data, and the use of cyberspace – an environment primarily employed for civilian purposes and governed by civilian entities – for military functions.

To untangle these complex legal matters, in 2009 the CCDCOE convened an international group of 20 noteworthy academics and practitioners. They undertook the task of producing a legal manual to explain how international law applies to the most severe cyber operations, allowing for self defense as well as those carried out during an armed conflict. Their work was published as the *Tallinn Manual* in 2013.

Yet, recognizing that states struggle every day with cyber operations that do not reach the armed attack threshold entitling them to act in self-defense, the CCDCOE has launched a follow-on endeavor titled "Tallinn 2.0." This project focuses on how international law regulates hostile cyber operations of lesser gravity that, nonetheless, cause states significant harm. That could include severe financial loss and the inaccessibility of vital online services. The project will also take an in-depth look at the obligations that international law places on states and how these apply in the cyber context, such as the duty not to knowingly allow one's territory to be used for acts that violate the rights of other states, and the prohibition of intervention into the affairs of other states. Once the project concludes in early 2016, the second expanded edition of the *Tallinn Manual* will be published. The manual will then cover the entire spectrum of international law applicable to state cyber operations in times of peace and war.

The center, in cooperation with the U.S. Naval War College and the NATO School Oberammergau, also contributes to the education of legal professionals by offering a profound course based on the *Tallinn Manual*. Taught by many of its key authors and information technology (IT) experts from the center who explain how cyber operations are carried out from a technical perspective, the International Law of Cyber Operations course runs twice a year and is open to all interested individuals.[2] It is vital for states that engage in cyber operations to educate their legal advisors. Other states should understand that so long as their cyber infrastructure is vulnerable to manipulation, once an attack materializes the need to comprehend the international legal implications of that situation arises. Therefore, training legal professionals on cyber matters is critical even in states where ambitions in cyberspace are limited. In today's security environment, states that rely upon cyber infrastructure must consider themselves susceptible to attack and prepare to handle them within the confines of international law.

In light of the growing investment in and overall attention toward cyber security, the Tallinn, Estonia–based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is attracting attention from NATO Allies to whom membership is open, and beyond.

COURSES AND EXERCISES

In addition to the International Law of Cyber Operations course, the center has developed an impressive portfolio of technical courses.[3] These delve into matters such as monitoring network traffic and logging security events, malware reverse engineering, and understanding how IT systems are attacked and how those attacks can be mitigated. Considering the high demand for these courses, attendance priority is given to students from the center's sponsoring nations. If vacant seats remain, they are offered to NATO nations and Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.

Each June, the CCDCOE organizes a major international cyber security conference called CyCon. Designed to inspire interdisciplinary discussion, the conference brings together more than 400 strategy, law, ethics and IT experts from the civilian and military sectors. Sessions run in two tracks and feature distinguished speakers (Estonian President Toomas Hendrik Ilves, known for his IT savviness and drive for technological developments, traditionally opens the event). CyCon provides a unique opportunity for professional exchanges and networking. In 2014, the theme of the conference in June was "active defense."[4]

Locked Shields, the center's real-time network defense exercise, is perhaps the most anticipated event of the year among participating security professionals. Twelve blue teams, each given access to identical, poorly configured networks shortly before the exercise commences, compete to determine who can best defend their network against cyber attacks by the red team. Just as in a sports competition, the exercise's three days are filled with excitement and competition, frustration and disappointment. But above all, Locked Shields is a unique learning opportunity for participants, requiring defenders to handle cyber attacks and maintain the functionality of the assigned networks under time pressure. The attackers, on the other hand, must discover alternative ways to target systems if the defenders repair vulnerabilities that were initially planned to be exploited (a skill that can be used when assessing the resilience of information systems against true hostile attacks). Moreover, Locked Shields tests the skills of legal advisors who analyze the ongoing cyber attacks in the context of the exercise's fictional scenario.

The militarization of cyberspace is a direct and inevitable consequence of societies' increasing reliance on information technology. It would be illogical to assume that states would not take advantage of cyberspace possibilities so long as they contribute to the accomplishment of national goals. As such, the notion of "cyber" is an unavoidable item also on NATO's collective security and defense agenda. The CCDCOE supports the Alliance by producing high-level research and training in a number of disciplines related to cyber security. As investments in cyber capabilities grow, so too will the role that the CCDCOE plays in helping to understand this domain. □

1. However, it is important to note that all COEs operate outside NATO's financial and command structure. For more on COEs, see Col. Andrew Bernard, "NATO Confronts Terrorism," *per Concordiam*, Volume 4, Number 3, pgs. 24-27, as well as NATO website at http://www.nato.int/cps/en/natolive/topics_68372.htm
2. For more information, including the dates of the courses, please visit http://ccdcoe.org/352.html
3. For a list of the course offerings and dates, please visit http://ccdcoe.org/236.html
4. For more information, please visit http://ccdcoe.org/cycon/2.html