BALTIC

Estonia, Latvia and Lithuania sign a historic document to align their cyber defense policies

CYBER COOPERATION

PER CONCORDIAM ILLUSTRATION

Vytautas Butrimas,

senior advisor, Cybersecurity and IT Department, Ministry of National Defense, Republic of Lithuania

It was a historic moment for regional cyber security cooperation when representatives of three Baltic countries — the minister of economic affairs and communications of Estonia, the minister of defense of Latvia and the minister of national defense of Lithuania signed a memorandum of understanding (MoU) on November 4, 2015. Three neighbors with a rich history of cooperation in traditional areas of defense recognized that they were also cyberspace neighbors and agreed to formalize the cooperation that had started informally several years prior. This article will discuss the process that led to the development of this new form of cyberspace cooperation, why the MoU is important and discuss some of its content. It will serve as a guide for other countries that wish to enter into similar agreements with their cyber neighbors.

THE ORIGINS

The idea for the cyber cooperation MoU emerged in late April/early May 2007, when NATO held a cyber security workshop hosted by the U.S. Department of Defense and Microsoft at the company's headquarters in Redmond, Washington. Participants learned of new possibilities for information technology use in defense for the then-new Microsoft operating system Windows Vista. Organizers announced that a Security Cooperation Agreement had been signed with China (later also with the Russian Federation) that allows its government access to Microsoft Windows source code.

But the mood of the conference changed dramatically as the next speaker, an Estonian, announced to the crowd that "my country is under cyber attack." Participants looked at each other with surprise and bewilderment. Here we were, in a NATO meeting with all the top cyber security officials present, and no one knew what to do. NATO had established no verified procedures to deal with a member state under cyber attack. No agreements, point-of-contact lists or mechanisms of coordination for assistance were in place to promptly react to this event. Later that evening, phone calls were made to capitals, and assistance was organized and provided to address the cyber attack underway in Estonia. Later, NATO developed and offered members the opportunity to sign MoUs for cooperation in cyber defense. Lithuania was one of the first to sign in the summer of 2010. The idea of the MoU took hold at the Lithuanian Ministry of National Defense, which also signed a local MoU with a national computer emergency response team (CERT) operated by the National Communication Regulatory Authority and later with the Ministry of Foreign Affairs. It became clear that it was a good idea to have a written agreement that could be drawn upon to handle future cyber incidents. This idea took root among the other Baltic countries as well.

HISTORY OF COOPERATION

In 2009, cyber security experts from the three Baltic countries met formally for the first time in Riga, Latvia. They subsequently agreed to meet regularly and rotate meeting locations among the three capitals. Cyber security experts from a wide range of institutions involved in securing the safety of cyberspace attended these meetings. In 2012, for example, the list of institutions represented included the three national CERTs and the ministries of transportation and communications, defense, foreign affairs, interior and police. It was decided as far back as 2010 to form a legal basis for these meetings in an MoU. The first working draft was prepared, discussed and modified in later meetings. This process went on for several years as personnel changed and national coordinating institutions for cyber security policy shifted to other institutions.

In Latvia, for example, the coordinating institutions changed from the Ministry of Transportation and Communications to the Ministry of Defense, while in Lithuania, the last alteration took place in January 2015, when the Ministry of National Defense was assigned responsibility for policy coordination, according to the Law on Cyber Security passed in December 2014. The last change provided stability in terms of institutional coordination, to finalize and ratify the MoU draft with each respective government and prepare for the official signing planned for the spring of 2015.

The official signing was delayed for several months, however, because of an additional requirement to make use of state of the art electronic signature technology. Many technical issues had to be overcome before the three national electronic signatures could be recognized by each signatory on the same document. Finally, after a great deal of work among the respective certificate authorities and institutions, on November 4, 2015, the Baltic ministers responsible for coordinating national cyber security policy signed the Baltic MoU for cooperation in cyber security.

WHAT IS IN THE MOU?

The Baltic MoU on cooperation in cyber security consists of statements on common beliefs that each nation shares and agreements on forms of cooperation among participating institutions. The "considering that" section lists these common beliefs:

- Information systems and networks are interconnected and interdependent both nationally and internationally.
- Governments and militaries are seeking cyber offense capabilities.
- Cyber threats emanating from cyberspace include cyber crime; nation-state attackers; cyber espionage; and politically, economically and/or socially motivated hacktivists.
- National security includes protecting information systems, computer networks, and critical infrastructure.
- To successfully address all of the above requires international cooperation.

Noteworthy among the stated beliefs is that cyber security is understood to be more than just dealing with the activities of cyber criminals and socially motivated hacktivists seeking to disrupt IT systems. The critical infrastructure that forms the foundation upon which modern society functions is also under threat from cyberspace. Cyber attacks that degrade the ability of control systems to monitor and control processes found in energy, transportation or water supply systems can harm the well-being of society, the economy and national security. That is why this infrastructure is called "critical."

The next section is the more concrete "agree to" part. There is nothing new here in

Baltic cyber experts meet in Riga, Latvia, in 2012.
VYTAUTAS BUTRIMAS

The Baltic cyber security cooperation memorandum of understanding is signed electronically during a video conference on November 4, 2015.

MINISTRY OF NATIONAL DEFENCE LITHUANIA

terms of Baltic cyber security cooperation; the activities listed in this section have been ongoing unofficially since the first meetings of Baltic cyber experts in 2009. The difference is that the MoU established a legal basis for the informal collaboration. Some of the activities include:

- Sharing knowledge and experience to develop domestic cyber security policies and practices
- Focusing on collaboration applicable to reducing risk and vulnerabilities associated with cross-border dependencies of interdependent information systems, networks and critical infrastructure
- Exchanging information about detected cyber incidents that can affect the cyberspace of other participating countries
- Sharing early warning information about potential attacks against another's information system or network
- Appointing points of contact (PoC) and exchanging contact information for regular and emergency communication

These points illustrate that a Baltic Cyberspace Community of Interest (BCCI) has been established to monitor, prevent and react to recognized cyber threats to each other's critical and information infrastructures. The appointment of a PoC is useful in that each party knows "who to call" in an emergency. Knowing the PoC in advance avoids confusion and potential difficulty when responding to cyber emergencies.

A NEW WAY OF SIGNING

The MoU could have been signed with traditional pen and ink followed by an exchange of fully signed copies. However, the electronic signature method using national identification cards was chosen. This was a good way to demonstrate technical cooperation and problem solving. It took several months to perfect the process in which different electronic signing software and standards could be applied and recognized by all parties.

While this trial and error problem-solving work was at times frustrating, it yielded a good thing: It provided an opportunity for Baltic countries to learn about each other's electronic signing technologies. Solving the issues enhanced the technical knowledge of each organization that could be used to make electronic signatures more popular among the Baltic countries in the future.

CONCLUSIONS

The signing of the MoU took more than five years to accomplish. Conceivably, it did not have to, but several factors contributed to making the process so lengthy. There are some lessons to be learned from the MoU process. First, it is always advantageous to meet and talk with cyber neighbors. It is often said that cyberspace "has no borders," which technically may be true but is not so in the electromagnetic reality of cyberspace. It makes sense to reach out to a neighboring country that has a physical border with you. You will find that you have much more in common in terms of cyber security than you may think. You will likely recognize that you are dependent on the same infrastructure for your nation's well-being. Electric grids, gas pipelines, fiber optic cables used in communications, and Internet links and transportation systems all cross cyber borders, making each neighbor dependent on the other in terms of providing and accessing critical services. A break in a cable providing links to international communications or a cascading failure in an electric grid affects not only the country where the fault originated, but may extend throughout the region.

A poem by Robert Frost called *Mending Wall* introduced the famous phrase "good fences make good neighbors." In the poem, each year two neighbors "meet to go down the line" checking and repairing the common wall that separates and forms the border between their two properties. The poet questions the need for a fence. One does not need to worry if his "apples" fall among the other neighbor's pine trees. However, the poet recognizes the need to deal with hunters crossing and damaging their lands. In today's cyberspace, cyber neighbors should "meet to go down the line" together to ensure each other's safety when dealing with threats to critical infrastructures emanating from commonly used and accessible cyberspace.

These are the structures that modern society depends on every day to function. The vulnerabilities and interdependencies of these structures cannot be secured by any one institution, but through cooperation with other interested parties. After a nation has first put its own cyber "house in order," signing an MoU with cyber neighbors is a practical first step for reducing risk and improving cyber security for everyone.

At the time of writing, there was a grand opening ceremony for new Lithuanian electric power links to Poland and Sweden. Critical infrastructure that includes power grids have both transborder and cyber dimensions, as IT-based control systems are used in electric power generation and distribution. With this latest event in mind, it is possible to foresee a need to expand the Baltic MoU to include two other cyber (and energy trading) neighbors of Lithuania: Poland and Sweden. □