Meeting of Cyber Defence Experts, January 2011

NATO

Estonia: Cyber Window into the Future of NATO

By HÄLY LAASME

For the development of the new North Atlantic Treaty Organization (NATO) Strategic Concept, a group of experts chaired by Madeleine Albright recommended that:

NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence.[1]

The Alliance has always adamantly protected its communications and information systems against harmful attacks and unauthorized access. Hence, until April 2007, the Atlantic Alliance had mainly concentrated on securing its own operational systems without realizing that it also should have been assisting its members in protecting theirs. As a result of the assaults on Estonian electronic infrastructure in April and May 2007, NATO changed its common security trajectory by extending the development of cyber defense capabilities also to its individual Allies.[2]

Häly Laasme is a Policy Analyst from Estonia. A graduate of Columbia University, she has conducted policy research for various Washington think tanks, including a panoptic research study of the European Defence Agency.

How did such a small nation end up as the driving force of the cyber defense policy of NATO? This article examines Estonia's role in the development of the NATO cyber defense policy, the adequacy of the current cyberspace concepts for defending NATO, and the Alliance's embracing of this new challenge with the help of the cyber center in Estonia.

Attack on e-Estonia

Estonia, a small country with a population of only about 1.3 million, is considered the most wired realm on the planet. Almost everything in this tiny nation, which gave birth to Skype, is done over computer networks and by use of mobile devices. Estonia ranks second in the world after the United Arab Emirates in mobile phone subscriptions, with each person in Estonia owning at least one device on average—188.2 devices per 100 people.[3] Almost every activity in Estonia is done over the Internet: its society is inundated with e-government, e-voting, e-parking, e-banking, e-identification systems, e-taxes, and live-streaming public television, to name a few.[4] Almost the entire country is covered by a free Wi-Fi network because Internet access is considered by Estonians as a basic human right. Estonia's pervasive Internet-driven culture is the realization of the dream of one man, Veljo Haamer, who wanted to make the Internet to Estonia what electricity is to the rest of the world.[5] As impressive as this extraordinary achievement is, it will soon be eclipsed by the European Union–supported €384 million project "EstWin," which aims to provide 100 megabits per second broadband service for every Estonian by 2015.[6] In summary, Estonia as an e-experiment is a window into the future for the rest of the NATO members and the world.

Unfortunately, this ubiquitous Internet dependence has brought not only technological freedom but also various defense and security risks. The national security of Estonia was threatened in April 2007 when a near-catastrophic botnet struck almost the entire electronic infrastructure of Estonia. Never before had an entire country been a digital target and the government forced to defend its population and commerce in cyber war. All that Estonian information technology (IT) managers could do was block the international connections to the servers, which was akin to a modern blockade of a country without the concomitant deployment of any conventional weapons.

Coincidentally, during the same time, three world-renowned IT experts were visiting Estonia, and they assisted the Estonian Computer Emergency Response Team with defenses against ping attacks, botnets, and hackers.[7] The experts were Kurtis Lindqvist, CEO of Netnod Internet Exchange, which operates one of the 13 Domain Name System's root servers in the world,[8] Patrik Fältström, senior consulting engineer with Cisco and cyber security advisor to the Swedish government,[9] and Bill Woodcock, research director of Packet Clearing House and member of the board of directors of the American Registry of Internet Numbers.[10] They happened to be at the right place at the right time to utilize their years of collective computer expertise and contacts among Internet service providers by sending out bursts of emails to the network operators around the world to block the Internet Protocol (IP) addresses that were sending harmful traffic to Estonia's international connections.[11]

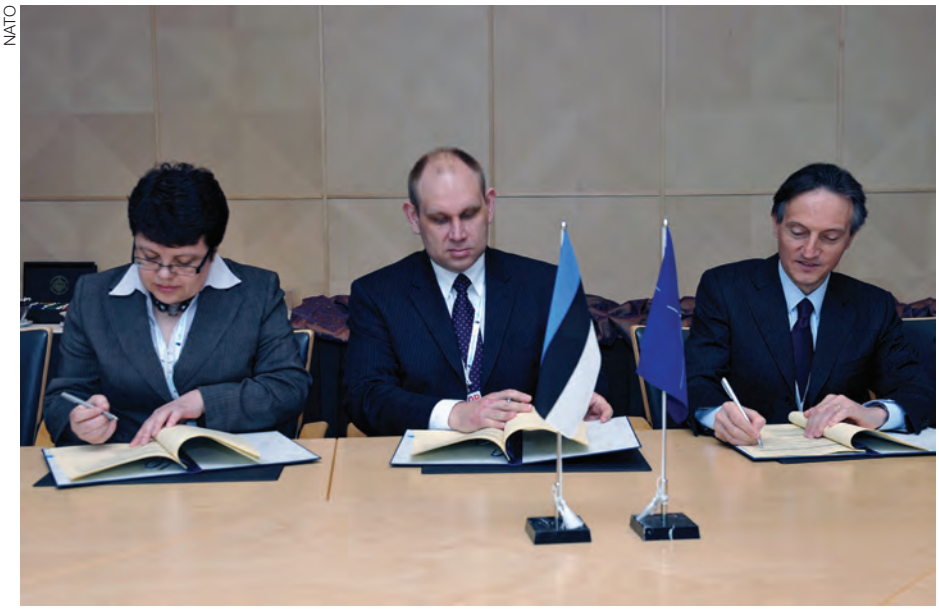
Ultimately, the country's electronic infrastructure was hit by almost one million computers simultaneously, most of them hijacked from the United States by unknown elements inside Russia.[12] The Russian government has denied any involvement with the attacks and has exhibited no interest in searching for the cyberterrorists who the evidence suggests were based in its country. What might be more troubling than the assault itself is that a group of Russian hackers has taken responsibility for it, implying that there exists a kind of private militia or stateless power[13] in Russia that can take down the commerce and government of any country in the world. Even though the Estonian case was not the first major cyber attack in the history of the Internet, it was the most publicized because it crippled an entire nation that is enormously dependent on network communications and offered empirical proof of hacking having evolved beyond the instrument of espionage.

almost the entire country is covered by a free Wi-Fi network because Internet access is considered by Estonians as a basic human right

Role of NATO

According to Article 5 of the NATO charter, an armed attack against any Ally is considered an attack against all. In such cases, Allies are called upon to assist each other with necessary measures, including the use of armed forces, to restore and maintain security.[14] Estonia has been a member of NATO since 2004, but in the case of the 2007 cyber attacks it could not invoke Article 5 because there was no agreed-upon enemy to retaliate against, and among Allies there existed ambiguity over what exactly constituted a weapon

NATO



NATO and Estonian representatives sign memorandum of understanding on cyber defense cooperation

under the Alliance's charter. This was a war in an absolutely different dimension; it was a virtual war that encompassed computers from all over the world.

Hitherto, NATO had not considered attacks by cyberterrorists as armed attacks. Accordingly, a collective self-defense was inapplicable, even though years earlier the Allies tested the charter with an "unfamiliar arsenal of weapons" by declaring the September 11 terrorist attacks with commercial airliners to be armed attacks and invoked Article 5.[15] But this might all change in the near future because NATO's new Strategic Concept includes cyber attacks as a significant threat to Euro-Atlantic security[16] that might warrant consultations under Article 4[17] and even lead to collective defense measures under Article 5 if necessary.[18] Furthermore, even if retaliation would have been justifiable, in this situation one could not have used conventional counterinsurgency strategies or tit for tat because there was no tangible theater of operations; the battlefield was cyberspace, and the identification of the enemy was quite ambiguous, not simply a defined number of computers from a certain country. In addition, this event raised another imperative ethical dilemma: if one cannot definitely prove the government of a particular country is the attacker, then should that government still be equally responsible for the hackers who attack another country? As anyone can infer, the area of "cyber defense and security" is still profoundly uncharted territory and its doctrine far from empirical realization. Neither in 2007 nor today are there any internationally accepted definitions on the subject of cyber defense and security. What one nation considers a "cyber attack" might appear more like a "cyber war" to another or even a simple "cyber crime" to a third.[19]

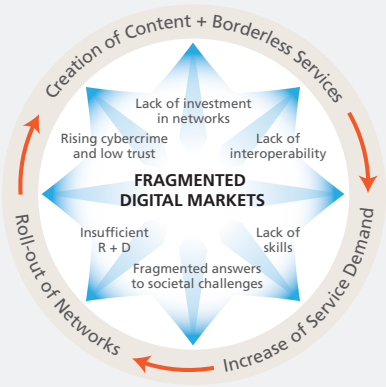
one could not have used conventional counterinsurgency strategies or tit for tat because there was no tangible theater of operations; the battlefield was cyberspace

Since 2001, the Council of Europe's Convention on Cybercrime has addressed the procedural laws in the signatory countries for investigating cyber crime while promoting cooperation in law enforcement, but it does not go beyond the basic necessities for solving identity theft or protecting intellectual property.[20] In October 2005, the United Nations Institute for Training and Research published Ahmad Kamal's *The Law of Cyber-Space*. The book describes in more detail different forms of cyber risks and notes that cyber war can occur between governments and nonstate actors, but nevertheless be financed by states.[21] This might have happened in the case of Estonia had there

NATO

Assistant Secretary-General for Emerging Security Challenges delivers opening statement at meeting of Cyber Defence Experts

Why a Digital Agenda for Europe?



Europe needs a new action plan for making the best use of information and communication technologies (ICT) to speed up economic recovery and lay the foundations of a sustainable digital future. The new action plan proposes to remove current obstacles to maximizing the potential of ICTs, with long-term investments to minimize future problems.

The Digital Agenda identifies where Europe needs to focus its efforts to put this virtuous cycle in motion. What is the focus of the Digital Agenda?

The Agenda outlines seven priority areas for action:

- creating a Digital Single Market
- improving the framework conditions for interoperability between ICT products and services
- boosting Internet trust and security
- guaranteeing the provision of much faster Internet access
- encouraging investment in research and development
- enhancing digital literacy, skills, and inclusion
- applying ICT to address social challenges such as climate change, rising health care costs, and aging populations.

been solid proof of the Russian government financing the hackers. The book also defines *cyber war* as "the deliberate use of information warfare by a state, using weapons such as electro-magnetic pulse waves, viruses, worms, Trojan horses, etc., which target the electronic devices and networks of any enemy state," and *cyberterrorism* as "attacks and threats of attack against computers, networks, and the information stored therein, with the objective of intimidating or coercing a government or its people in furtherance of political or social objectives."[22] De facto, there is only one distinction between these definitions: the classification of the conspirator as state or nonstate. Hence, cyberterrorism can evolve into cyber war if the state finances the terrorists. But even if the quarreling parties have been identified, there still exists a jurisprudence dilemma because unlike the international trade disputes that can be filed with the World Trade Organization, there is no such globally recognized entity or appellate body for cyber conflicts. Every country is on its own on translating how the domestic and international laws cover the different actions in the cyber world and how to penalize the mischievous cyber-citizens. This problem has become highly relevant again because of the recent Internet publication by WikiLeaks of U.S. diplomatic cables. This action has in the short term more or less flabbergasted the U.S. Department of Justice over how exactly to discipline such deeds.

To progress with advancing technologies, in 2002 the Alliance included development of cyber defense capabilities in its agenda and established the NATO Computer Incident Response Capability (NCIRC) as part of the newly implemented Cyber Defence Programme.[23] In 2008, after 6 years of labor in bringing the NCIRC up to full operational capability, the Alliance's member states ratified the NATO Cyber Defence Policy and created the Cyber Defence Management Authority in Brussels, all prompted by what had happened almost a year earlier to Estonia. NATO finally realized that some form of common strategy had to be developed for defending the electronic infrastructures of its member states. Nevertheless, it still took 2 more years for the Alliance to make a contribution to the development of a global cyber-lexicon. On January 22, 2010, NATO finally defined in its glossary the term *computer network attack* as "Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself" and noted that "a computer network attack is a type of cyber attack."[24] However, the definition still lacks a ranking of offenses for identifying the severity of an attack: whether it should be considered as just a sophisticated and malicious hacking or as an act of war that requires retaliation by allies, and then what kind of counterinsurgency strategies would be adequate. Unfortunately, NATO's new Strategic Concept has not contributed much toward clarifying these ambiguities for the Allies. Even though it might not be NATO's mission to classify and define everything in cyberspace, it is the Alliance's role to prevent crises, manage conflicts, and defend one another against attacks, including against new threats—none of which can be conducted with vague directions and abstruse concepts. In the global context, this means that the role of NATO in defining cyberspace concepts and linking them to the applicable and tangible counterinsurgency strategies should be considered as pertinent as was the redefining of the post–Cold War security environment.

NATO

Estonian president meets with Secretary-General at NATO Headquarters

The Cooperative Cyber Defense Centre of Excellence

The cyber incident with Estonia was a wake-up call for the Alliance. After an all-inclusive evaluation of its cyber defense capabilities, in May 2008 Estonia, Italy, Spain, Slovakia, Germany, Lithuania, Latvia, and the Allied Command Transformation signed a memorandum of understanding for the establishment of a Cooperative Cyber Defence Centre of Excellence (CCDCOE) in the Estonian capital, Tallinn.[25] This was the 10th Center of Excellence accredited by NATO, and its aim has been to enhance the Allies' capabilities and interoperability in cyber defense by emphasizing doctrine and concept development, awareness and training, research and development, analysis and lessons learned, and consultations.[26] Given that the CCDCOE does not belong to the NATO command structure, its capital and administrative costs are covered by the host country, Estonia, while the rest of the expenses and operating costs are shared by all the sponsoring states.[27] In June 2010, Hungary joined the Centre as a sponsoring state, and the United States and Turkey have both shown great interest in joining in the future.[28] Considering the increased involvement of U.S. experts in the activities of the CCDCOE, membership might not be too far off.

Since its establishment, the CCDCOE has worked vigorously to educate its members on cyber security issues and has already organized several cyber defense conferences. In June 2009, it sponsored the first international Conference on Cyber Warfare, where speakers from 13 countries delivered 29 cyber warfare presentations. During the 3-day event, besides various other subjects, participants received analysis on China's intelligence collection network, GhostNet, which had infiltrated high-level computers in more than 100 countries, including an unclassified

computer at NATO headquarters;[29] on measuring techniques of distributed denial-of-service attacks; on the concept of borders in cyberspace; and on botnet countermeasures.[30] The conference was the first clear indication of the intent of NATO and its Allies not to dawdle, but to consider every aggression in cyberspace seriously. Similar to the Russian hackers who assaulted Estonian electronic infrastructure, the Chinese government has denied any involvement with Chinese hackers who operate GhostNet. Yet this is another example of groups of sophisticated programmers who are capable of hacking into computer systems around the world becoming a more prevalent and serious security issue. NATO members have started to realize that in managing cyberspace, any kind of vulnerability can lead to dangerous consequences in defense, even when the hackers' aim might be only economic espionage to acquire cutting-edge technology or scientific know-how.

Various security problems can be solved and offensive strategies created by hiring capable and seasoned programmers. In 2007, Estonia was extremely lucky in finding three highly experienced IT talents in country who were ready to apply their efforts on Estonia's behalf, but in reality many companies and countries do not have such experts sitting around to protect their servers. Therefore, security issues have to be tackled long before they become dangerous, and explicit procedures for dealing with consequences must be defined. In brief, we need an internationally accepted body of principles and rules to govern cyber affairs and conflicts—cyberspace's very own ex ante and ex post regulations. Global policies and laws are lagging decades behind the fast-advancing technologies. As the director of the CCDCOE, Colonel Ilmar Tamm, has noted, "Even if some means to secure the cyber domain are technologically feasible, we are limited by laws and policies."[31]

Consequently, the CCDCOE progressed even more swiftly in educating the Allies by hosting a second cyber security symposium, Cyber Conflict Legal and Policy Conference, in September 2009. The event, which was organized jointly with the George Mason University Center for Infrastructure Protection, explored rules and regulations in cyber conflict management.[32] This debate is not just vital but also highly sensitive because people who use the Internet generally believe that it will be incredibly challenging to manage and balance any policies and laws in the open environment of cyberspace without infringing on its current innate premise—client/user equality—that essentially makes the World Wide Web so powerful for its users.

For NATO, it does not matter if the theater of operations is cyberspace or conventional terrain; the success of operations still depends on the asymmetry of information. Meanwhile, preservation of international security in the nonvirtual world sometimes necessitates offensive strategies for avoiding extensive collateral damage in the long run; on the other hand, achieving security in the cyber world often entails more defense strategies because presently tracking down the dynamic IP addresses and retaliating appropriately are more complicated processes than well-prepared cyber deterrence. To advance members' cyber defense capabilities, in May 2010, the CCDCOE, together with the NCIRC, organized the 13th NATO Cyber Defence Workshop and in October 2010, it co-hosted with Allied Command Transformation a workshop called NATO in the Cyber Commons, which was strictly aimed at identifying the Alliance's vulnerabilities and developing relevant capabilities.[33]

even if some means to secure the cyber domain are technologically feasible, we are limited by laws and policies

Dual-use Technology

The CCDCOE emphasizes the need for collaboration in research between various military and civilian entities. On November 3, 2009, the Centre signed a 3-year research cooperation agreement with one of Northern Europe's leading financial groups, SEB (Skandinaviska Enskilda Banken), to explore the best practices of information-securing in the private sector,[34] and on January 11, 2010, Symantec Corporation announced its participation in the collaborative study that is expected to address the threats that undermine online systems.[35] Although Symantec's engagement in international security issues should be highly welcomed, de facto, the sophistication of the hacking community has evolved beyond this NASDAQ–100 company's capability. According to its consumers, Symantec's capability seems to be struggling with engineering constructive solutions for its customers whose computers have been infected with malware containing a backdoor component while being protected by Symantec security products.[36]

Information technologies are developing beyond the pace of our collective ability to provide secure defense. While computers and thousands of software applications for mobile devices make our daily lives more efficient, they also lead to more complex cyber defense issues.

Almost everything in our electronic infrastructure is a dual-use technology that has applications for military operations as well as for civilian tasks like operating systems, security software, and networking protocols. Many commercial applications and interfaces were originally developed under defense research, including the Internet. It is cost-effective and profitable to develop dual-use technologies because demand in the military market is much smaller than in the commercial market.

In cyberspace, the most imperative dual-use technologies are products based on cryptography. It has become increasingly obvious that the protection of critical infrastructures necessitates strong encryption capabilities.[37] The encryption and decryption algorithms allow secure messages to be sent between defense and security entities as well as between civilians by common interfaces like Blackberries. Therefore, developments in these kinds of dual-use technologies require high vigilance from defense and commercial consumers and inclusive collaboration among all pertinent parties.

Estonia became the driving force of NATO's cyber security policy because its citizens dependence on technology in their everyday lives was greater than the other Allies. With the 2007 cyber war, Estonia experienced firsthand how unprepared NATO was to defend its members in this new reality. Thus, calling for a NATO common cyber security policy was the only option for defending the country against future cyber attacks because, in foreign policy, intentions to do something can often work as deterrents. Since there have been no major cyber attacks on the country during the last 3 years, it does seem like this strategy has worked. Now that NATO's Strategic Concept has been developed, it is vital to comprehend the array of new challenges that cyberspace imposes on the Alliance. Estonia

can be an excellent case study for NATO, which needs to continue to learn from the Estonian example and incorporate cybersecurity in its charter and mutual defense doctrines. Cooperation in advancing cyber defense capabilities is becoming more relevant and critical because it is almost impossible to defend any country's electronic infrastructure solely with its own resources, as the cyber attacks on Estonia demonstrated. The few international policies that regulate cyberspace only concentrate on commercial and civilian matters to protect minors from indecent exposure, citizens from identity theft, and corporations from loss of profits.

Meanwhile, cyber defense issues have not been effectively discussed and the actions for solving possible consequences not defined. Utilizing the Cyber Defence Centre in Estonia is a highly efficient way for NATO to begin confronting the defense challenges posed by the cyber world, but it will not be effective for the Alliance when faced with the profound combination of challenges that the prevailing trend of increased dilemmas seems to suggest the cyber future will bring. Until now, NATO members and the developed countries have dealt with isolated cyber attacks. But what if these assaults evolve into something much more serious, like purposely shutting down nuclear and hydropower plants, taking down satellites, or stealing and publishing something considerably more sensitive and classified than WikiLeaks has done? **JFQ**

NOTES

[1] North Atlantic Treaty Organization (NATO), "Strategic Concept: NATO 2020: Assured Security; Dynamic Engagement," May 17, 2010, 12, available at <www.nato.int/strategic-concept/expertsreport.pdf>.

[2] NATO, "Defending Against Cyber Attacks: How Did the Policy Evolve?" January 29, 2009, available at <www.nato.int/issues/cyber_defence/index.html>; NATO, "Addressing the Technical and Political Aspects," March 31, 2008, available at <www.nato.int/issues/cyber_defence/practice.html>.

[3] World Economic Forum and INSEAD, "The Global Information Technology Report 2009–2010," March 25, 2010, available at <www.networkedreadiness.com/gitr/main/>.

[4] Republic of Estonia, "e-Estonia," available at <www.valitsus.ee/?id=5450>.

[5] Indrajit Basu, "Estonia Becomes E-stonia," *Government Technology*, April 9, 2008, available at <www.govtech.com/gt/284564?topic=117673>.

[6] European Union, "State Aid: Commission Approves State Aid for High Speed Internet in Estonia," press release, Brussels, July 20, 2010, at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/975&format=HTML&aged=0&language=EN&guiLanguage=en>.

[7] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine* 15, no. 9 (August 2007), available at <www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1>.

[8] Internet Society, "The Seven Stages of IPv6 Adoption: Panelist," March 24, 2009, available at <www.isoc.org/isoc/conferences/ipv6panel/>.

[9] European Union, "The 2d Annual Internet of Things Europe 2010, A Roadmap for Europe: Speaker," June 1, 2010, available at <www.eu-ems.com/speakers.asp?event_id=55&page_id=348>.

[10] Organisation for Economic Co-operation and Development, "ICT4D: Speaker," September 10, 2009, available at <www.oecd.org/speaker/0,3438,en_21571361_42740239_43635974_1_1_1_1,00.html>.

[11] Davis.

[12] Ibid.

[13] Ibid.

[14] NATO, "What Is Article 5?" February 18, 2005, available at <www.nato.int/terrorism/five.htm>.

[15] Ibid.

[16] NATO, "New Strategic Concept: Active Engagement, Modern Defence," November 19, 2010, 4, available at <www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.

[17] According to the North Atlantic Treaty, Article 4 states, "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened." NATO, "The North Atlantic Treaty," December 9, 2008, available at <www.nato.int/cps/en/natolive/official_texts_17120.htm>.

[18] NATO, "Strategic Concept: NATO 2020: Assured Security; Dynamic Engagement."

[19] Estonian Ministry of Foreign Affairs, "Estonia and NATO Article Five," *Glance at the Mirror 2008*, February 23, 2009, 6, available at <http://web-static.vm.ee/static/failid/238/NATO_art5.pdf>.

[20] Council of Europe, "Convention on Cybercrime," November 23, 2001, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>.

[21] Ahmad Kamal, *The Law of Cyber-Space* (New York: United Nations Institute for Training and Research, 2005), 81, available at <www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf>.

[22] Ibid., 13.

[23] NATO, "Defending Against Cyber Attacks: NATO Cyber Defence Policy and Activities," October 28, 2010, available at <www.nato.int/cps/en/natolive/topics_49193.htm>.

[24] NATO Standardization Agency, *NATO Glossary of Terms and Definitions*, Allied Administrative Publication 6, March 22, 2010, 70, available at <www.nato.int/docu/stanag/aap006/aap-6-2010.pdf>.

[25] NATO, "NATO Opens New Centre of Excellence on Cyber Defence," *NATO News*, May 20, 2008, available at <www.nato.int/docu/update/2008/05-may/e0514a.html>.

[26] NATO, Transformation Network, "Cooperative Cyber Defence (CCD) COE (Estonia)," July 2009, available at <https://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD>.

[27] Ibid.

[28] Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Hungary Joins the Centre," *CCDCOE News*, June 23, 2010, available at <www.ccdcoe.org/188.html>.

[29] Ron Deibert and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor* (March 2009), available at <www.news.utoronto.ca/media-releases/international-affairs/information-warfare-monitor.html>.

[30] CCDCOE, "Conference on Cyber Warfare," 2009, available at <www.ccdcoe.org/cyberwarfare/3.html>.

[31] CCDCOE, "President of Estonia Opened International Cyber Conflict Legal and Policy Conference," September 9, 2009, available at <www.ccdcoe.org/legalconference/311.html>.

[32] CCDCOE, "Cyber Conflict Legal and Policy Conference 2009," available at <www.ccdcoe.org/legalconference/3.html>.

[33] CCDCOE, "NATO in the Cyber Commons," *CCDCOE News*, October 19, 2010, available at <www.ccdcoe.org/199.html>.

[34] CCDCOE, "CCDCOE Signs Agreement with SEB," *CCDCOE News*, November 5, 2009, available at <www.ccdcoe.org/155.html>.

[35] CCDCOE, "Symantec and Cyber Defence Centre of Excellence Experts to Research Online Threats," *CCDCOE News*, January 11, 2010, available at <www.ccdcoe.org/7.html>.

[36] Symantec, "Forum Discussions, Blog Entries, Articles," available at <www.symantec.com/connect/search/apachesolr_search/backdoor>.

[37] Jay Stowsky, "Secrets to Shield or Share? New Dilemmas for Military R&D Policy in the Digital Age," University of California, July 28, 2003, 6, available at <http://socrates.berkeley.edu/~scotch/stowsky.pdf >.