NEW VOICES
IN PUBLIC POLICY

Volume VII

Spring 2013

Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success

Camille Marie Jackson

GEORGE MASON UNIVERSITY | School of Public Policy

ISSN: 1947-2633

On Friday, April 27, 2007, a number of Estonian government officials could not access their e-mail at work. Microsoft Outlook-based systems were not able to send or receive e-mail, and overall network connectivity slowed.[1] Such incidents are fairly common and generally short-lived, and many Estonian officials thought the error would be fixed in a few minutes or hours. However, as days and weeks wore on, it became apparent that Estonia was under a serious cyber attack—or rather a series of attacks---which had significant economic, political, and security consequences for this tiny, technologically-dependent Baltic country.

The cyber attacks of Spring 2007 sparked a series of dramatic policy changes designed to make Estonia's networks more secure, ranging from adjustments to the legal code to the creation of a Cyber Security Strategy and Cyber Defense League.[2] For the remainder of this case study, we will examine the forces driving these policy changes, as well as the special cultural and political dynamics at play that allowed particular proposals to come to fruition. We will then look at the policies that were adopted, and assess the success of these measures.

It is important to understand that the cyber attacks on Estonia coincided with an intense political conflict with Russia. After Estonia regained its independence from the Soviet Union in 1990, it began a process of modernization and de-Sovietization—a course that sometimes created tension among the ethnic Russian minority living in Estonia.[3] [4] Their concern reached a climax in April 2007, as Estonian officials were debating whether to move a controversial bronze Soviet statue located in Tallinn, the Estonian capital. To the ethnic Russian minority, this statue was a symbol of their legitimacy and rights in Estonia.[5] But for some Estonians, it represented a brutal Soviet takeover of their country, and in 2006 these citizens petitioned the Tallinn City Council to demolish the monument.[6] Spurred by growing protests on both sides, on April 26 and 27, 2007

the controversy spiraled into deadly rioting and looting, and the Estonian government decided to dismantle the bronze statue to close the matter and dispel the rioting. [7]

It was within this framework that the cyber attacks took place, beginning on April 27, 2007. On April 29, hackers hit the ruling Reform Party's webpage and posted a message indicating that the Estonian Prime Minister had sought forgiveness from Russia and promised to return the statue.[8] Hackers manipulated other websites to redirect visitors to pictures of Soviet soldiers or quotations from Martin Luther King Jr. about resisting "evil."[9]

Additionally, a significant portion of Estonian government, banking, and media websites were inundated with Distributed Denial of Service (DDoS) attacks, preventing them from communicating via e-mail or conducting business transactions. The scope, sophistication, and duration of these attacks were unprecedented, according to US scholars.[10]

The cyber attacks on Estonia had a significant impact in part because Estonian society is so heavily dependent upon modern information systems. In a meeting with President George W. Bush in June 2007, then-President of Estonia Toomas Ilves noted that "it is a serious issue if your most important computer systems go down in a country like mine, where 97 percent of bank transactions are done on the Internet. When you are a highly 'Interneted' country like we are, then these kinds of attacks can do very serious damage."[11]

In addition to Estonian banks' heavy reliance on online transactions, the country's e-Government system also makes it particularly vulnerable to cyber attacks. E-Government is a system that uses the Internet to make government goods, information, and services available to citizens and businesses.[12] According to Kristina Reinsalu, program director at the e-Governance Academy, Estonia's use of e-Government systems to conduct transactions is "remarkably high," and Estonia ranks first among new members states in the EU for the use of such systems.[13]

These vulnerabilities made the cyber attacks particularly crippling, and basic government functions were adversely affected for weeks. As the attacks continued, Tallinn eventually decided to cordon the nation's networks off from international servers, isolating the country's systems to allow them to recover.[14] As a result, during this time Estonian computer networks were cut off from the outside world—a solution that served to block the attacks, but created additional connectivity problems. For example, although Estonians could access their e-mail and online services within Estonia, those travelling abroad could not access e-mail or banking services.[15]

The Estonian networks were finally re-established after several weeks, and reconnected to foreign servers in late May 2007, a month after the initial attacks.[16] Yet an obvious task remained: how could Estonian officials prevent such an attack from happening again in the future?

According to Kristjan Prikk, an Estonian diplomat who was stationed at the Ministry of Foreign Affairs when the attacks occurred and at the Ministry of Defense as many new policies were being implemented, four unique forces provided the impetus for Estonia's new cyber policies: the country's heavy dependence on information technology; the fact that a number of new policy ideas had already been introduced, but not implemented; strong support from the public and industry to implement changes; and a unified vision within the Estonian government.[17]

First, Estonia's heavy dependence on information technology is central to explaining the changes in the country's cyber policies. Estonia's heavy use of information technology is part institutional and part cultural. Over the past twenty years, the Estonian government has invested significant resources into modernizing the country's infrastructure,[18] creating institutions and

policies to bring Estonia more fully into the twenty-first century, and connecting it more closely with the rest of the world.

At the same time, as political scientist Francis Fukuyama has noted, "institutions reflect the cultural values of those in the country in which they are established."[19] The information technology systems that have appeared in Estonia cannot necessarily appear anywhere—Estonia has a unique culture that is open to these establishments, that is willing to do 97 percent of all banking transactions online, and that is willing to sacrifice some privacy in exchange for efficiency, convenience, and modernity.[20] According to Linnar Viik, a professor at the Estonia IT College, information technology is a way of life in Estonia, and "this way of life and the values of society aren't controlled by state ministries of defense. They are supported by culture, education, the economy."[21] Because of this unique blend of culture and institutions, Estonia became a prime location for new, sweeping information technology policies to take hold.

Second, in addition to this information technology culture, a number of initiatives to increase Estonian cyber security had already been introduced within the government, but not yet adopted. In John Kingdon's conceptualization of the policy-making process, solutions to policy problems are often devised long before the problems arise. [22] Then, he argues, policy "entrepreneurs" lie in wait until a policy window opens, at which time they have an opportunity to couple their solution to a particular policy problem.[23] The 2007 Attacks were that window. When the cyber attacks struck, Estonian officials had a variety of ideas to choose from and implement; initiatives such as the Cooperative Cyber Defense Center of Excellence (CCDCOE) and the Estonian Cyber Defense League.

Third, there was strong support from the both the Estonian public and industry to increase cyber security. According to Mr. Prikk, as Estonian officials were considering and making new

policy, "The top political leadership was interested in seeing new policies succeed, while people in the private sector [had] trust; the drive for doing something was everywhere."[24] Before the 2007 Attacks, most of the major banks in Estonia were owned by foreign—primarily Swedish—banks. This ownership structure encouraged Estonian banks to integrate their institutions more closely with the Swedish banks, including hosting servers on Swedish territory. However, after the 2007 attacks, it became apparent that the presence of Estonian banks' servers on Estonian soil was essential for the banks' ability to protect themselves and quickly recover from an attack. As a result, the government began instituting regulations on which banks' and other critical businesses' servers could be hosted, as well as the size of data storage. Estonian banking firms, which had been hit hard by the cyber attacks, supported government efforts to make their networks more secure. [25]

Fourth, Mr. Prikk also noted a sense of unity within the Estonian government, which acted as an added impetus for policy change.[26] This factor is comparable to the momentum that propelled the US Congress and the White House to pass new legislation and make significant changes to US homeland security policy following the September 11 Attacks. According to Mr. Prikk, "the interconnectedness between the people and the institutions was the greatest achievement. . . . This was not necessarily a top-down approach or a bottom-up approach, but it was an inclusive approach. Not just a whole of government approach, but a whole of nation approach."[27]

Out of the 2007 Attacks emerged a sense of unity, a sense that all elements of the government infrastructure—working together—were necessary to combat the cyber threat. Phillip Bobbit reflects this general idea in his book *The Shield of Achilles* by noting that:

> For the first time since the birth of the State, a state structure is no longer necessary to organize violence on a scale that is devastating to society. And yet, perhaps ironically, this development makes the role of the State all the more crucial in achieving international peace and national security. This is because the shift away from retaliatory, threat-based strategies to defensive, vulnerability-based strategies will require a State—indeed will require a society of states—to successfully execute.[28]

With these four forces driving the Estonian government to enact new policies to secure its infrastructure, Estonia chose to implement several new policies. Czosseck, Ottis and Taliharm outline Estonia's most salient policy changes in a 2011 paper released by the Cooperative Cyber Defense Center of Excellence (CCDCOE).[29] Because of the large number of changes implemented by the Estonian government, for the purposes of this paper we will discuss only three below: the creation of a Cyber Security Strategy, the CCDCOE, and the Cyber Defense League. (For additional policy changes, see Appendix A.)

First, the creation of Estonia's Cyber Security Strategy has been heralded as "the most significant step" in the country's cyber security response.[30] Released in May 2008, the Strategy was created by a multi-agency council led by the Ministry of Defense, and identified five strategic objectives: developing and implementing a system of security measures, increasing competence in information security, developing a legal framework for cyber security, developing international cooperation, and raising cyber security awareness.[31] Estonia's Cyber Security Strategy has become the guiding document for the state's comprehensive cyber policy, [32] and has been a driving force for additional changes.

Second, the creation of the CCDCOE was a significant policy change and, as with a number of initiatives implemented by the Estonian government, had its beginnings well before

the April 2007 attacks.[33] In 2003, even before Estonia joined NATO, the country recommended the creation of a new "center of excellence" for telecommunications security within the NATO framework.[34] Despite general support from NATO leadership, the idea did not gain momentum until after the 2007 attacks, when it received significant support and finally came to fruition in May 2008. According to a press statement on the CCDCOE's website, "the [CCDCOE] is a NATO accredited international military organization with aim to enhance cooperative cyber defence capabilities of NATO and NATO nations."[35]

The CCDCOE is not an active cyber force or a cyber control center—rather it is an international research consortium meant to increase international awareness and understanding of information security best practices. Though seemingly unimpressive, within this consortium Estonia is able to promote international cooperation to solve cyber security problems—a multinational focus that Estonian officials maintain is necessary for success in the cyber security realm.[36]

A third institutional and policy change was the creation of a Cyber Defense League in 2010. The league is made up of information technology specialists who volunteer to assist the Estonian military during a time a crisis. The Cyber Defense League is made up of small, locally operated units. Prior to 2010, these volunteers worked loosely together to defend Estonian networks, and the creation of an Estonian Computer Emergency Response Team (CERT) in 2006 as well as new policies on information sharing increased collaboration between these groups. However, after the 2007 Attacks Estonia decided to nationalize this unit so that it could more effectively and cohesively defend the country during a cyber attack.[37]

According to Mr. Prikk, a strong public desire to reach out and help was key to creating the Cyber Defense League. "Whenever there is a big crisis," he said, "there are always people

who…will to do something for the country."[38] Many Estonian citizens self-mobilized following the 2007 Attacks. Some helped in more immediate and visible ways, joining the police reserve force and helping to quell rioting in the streets. A second wave of volunteers responded cyber attacks, as individuals with computer technology skills decided that they, too, would like to help their country.[39] By forming the Cyber Defense League, the Estonian government was able to harness this desire and channel it in a comprehensive, constructive fashion.

Having examined the driving forces that led Estonia to adopt a series of new cyber policies, we will now examine the effectiveness of these new measures. Cyber policy is a relatively new area of public administration, and because Estonia's policies are still new and untried, our ability to accurately judge the effectiveness of these measures are limited. However, by examining three criteria—assessments by experts, whether other countries have followed Estonia's lead, and whether Estonia has successfully defeated additional attacks—we can reach a general estimate of the policies' success.

A number of academics and experts have given general, overarching assessments of Estonian information security policies. Czosseck, Ottis and Taliharm approve of Estonia's rapid development of its Cyber Security Strategy by noting that these policies are a "significant step" and recommend that other countries adopt their own cyber security strategy.[40] Further praise for Estonian policies comes from Dr. Lene Hansen and Dr. Helen Nissenbaum, researchers at the University of Copenhagen and New York University, respectively. They note that Estonian officials were successful in garnering support for cyber security and implicitly give credit to the Estonians for driving forward NATO's cyber policy, including the creation of the CCDCOE.[41] Legal scholar Scott Sheckelfield praises the short-term response of the Estonian Cyber Emergency Response Team (CERT) for ultimately prevailing against the attacks; but believes an

international treaty in needed to clarify appropriate responses and prevent future cyber attacks.[42] In general, the literature on Estonian cyber policies is positive, although no author has come out with a categorical assessment of all Estonian national information security policies since 2007.

Estonia's adoption of a comprehensive cyber strategy and similar initiatives undertaken in neighboring countries provides the best example of how various nations are following Tallinn's lead. Since Estonia released its Cyber Security Strategy in May 2008, a number of European countries have released similar strategies, including Germany, the Netherlands, France, and the United Kingdom.[43] [44] [45] [46] It is impossible to prove that Estonia's Strategy was the central catalyst for these new policies, and, indeed, the United States released its own Comprehensive National Cyber security Initiative in January 2008—four months before the release of Estonia's document.[47] However, the proliferation of national cyber security strategies shows that many countries are reaching the same conclusion: it is in a nation's best interest to develop a comprehensive strategy to secure information networks. Estonia was one of the first nations to adopt such a Strategy, and continues to lead the way in promoting this trend.

We can also measure the effectiveness of Estonian policies by observing the extent to which these measures have protected Estonian networks from additional attacks. There have not been any significant computer network breaches reported in Estonia since the 2007 Attacks. The Estonian Information System's Authority website refers only to the 2007 Attacks when noting the incidents they have addressed.[48] However, a lack of visible evidence for a cyber attack is not necessarily evidence of success for Estonian cyber policies. It is possible for the Estonian government to hide breaches of its networks, or significant attacks may have not yet tested the new infrastructure and policies in place. However, available evidence suggests that Estonia has

not suffered any debilitating attacks on the same scale as the 2007 incident. If used as one metric among various criteria, we can conclude that these new policies have been successful.

It is too early to judge the full effectiveness of Estonia's policies since the 2007 Attacks. However, the forces driving these policy changes have become clear: the country's heavy dependence on information technology; the underlying, existing groundwork for a number of these policies; strong support from both the public and industry; and a unified vision and impetus within the Estonian government. These forces suggest that the changes which have taken place in Estonia over the past four years are unique given its culture and position. However, other countries are already mimicking some of Estonia's new policies, and Tallinn's initiatives may continue to set precedents as cyber security becomes more important in world affairs.

---

[1] Based on a personal interview with Mr. Kristjan Prikk, currently an Estonian diplomat stationed in Washington DC, and in April 2007 stationed at the Ministry of Foreign Affairs in Tallinn, 21 November 2011.

[2] Christian Czosseck, Rain Ottis and Anna-Maria Taliharm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security." Cooperative Cyber Defense Center of Excellence Website, 2011. http://www.ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF.

[3] Raphael Shen. *Restructuring the Baltic Economies: Disengaging Fifty Years of Integration with the USSR*. 1994. London: Praeger Westport, 1-2.

[4] Marju Lauristin and Mati Heidmets. *The Challenge of the Russian Minority: Emerging Multicultural Democracy in Estonia*. (Talinn: Tartu University Press, 2002), 31-54.

[5] Aleksandr Daniel, "Российский историк: Проблема в том, как жить рядом двум народам с такой разной исторической памятью," (Russian Historian: The Problem Is How Two Nations Live Close Together with Such Different Historical Recollections), Regnum, 4 May 2007.

[6] "Estonian Nationalists Want Statue of WWI Soviet Liberator in Tallinn be Pulled Down," Kommersant, 8 May 2006. At http://www.kommersant.com/p-8583/r_500/Estonian_Nationalists_Want_Statue_of_WWII_Soviet_Liberator_in_Tallinn_be_Pulled_Down/.

[7] "Tallinn Tense After Deadly Riots." *BBC News.* 28 April 2007. http://news.bbc.co.uk/2/hi/europe/6602171.stm.

[8] "The Cyber Raiders Hitting Estonia," *BBC News*, 17 May 2007. http://news.bbc.co.uk/2/hi/europe/6665195.stm.

[9] Ibid.

[10] Franklin D. Kramer, Stuart H. Starr, and Larry Wentz. *Cyberpower and National Security*. (Washington DC: National Defense University Press 2009). 14.

[11] Anne Broache, "Bush, Estonian President Talk Cyberattacks," CNET, 25 June 2007. At http://news.cnet.com/8301-10784_3-9734382-7.html.

[12] United Nations Department of Economic and Social Affairs. United Nations e-Government Survey 2010: Leveraging e-government at a Time of Financial and Economic Crisis (New York: UN Publishing Department, 2010), 2.

[13] Kristina Reinsalu, "Is Estonian Local E-Government Responsive to Citizens' Needs? The Case Study of Tartu," Information Policy: The International Journal of Government and Democracy in the Information Age, 11, no. 3,4 (2006), 256.

[14] Prikk

[15] Prikk

[16] Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," Berkeley Journal of International Law 27 no. 1 (2009), 205.

[17] Prikk

[18] John Borland, "Perspective: Estonia Sets Shining Wi-Fi Example," CNET, 1 November 2005. At http://news.cnet.com/Estonia-sets-shining-Wi-Fi-example/2010-7351_3-5924673.html .

[19] Francis Fukuyama, The Origins of Political Order: From Prehuman Times to the French Revolution (New York: Farrar, Straus and Giroux, 2011), 14.

[20] Prikk

[21] Isabelle de Pommereau. "Why Estonia May be Europe's' Model Country." *Christian Science Monitor*. 18 May 2011, http://www.csmonitor.com/World/Europe/2011/0518/Why-Estonia-may-be-Europe-s-model-country.

[22] John Kingdon, Agenda's Alternatives, and Public Policies, 2nd ed. (New York: Longman, 2003), 181-190.

[23] Kingdon, 181-190.

[24] Prikk

[25] Prikk

[26] Prikk

[27] Prikk

[28] Phillip Bobbit, *The Shield of Achilles: War, Peace, and the Course of History* (New York: Random House, 2002), 806.

[29] Czosseck, et. al., 57-64.

[30] Czosseck, et. al., 61

[31] Estonian Ministry of Defense. Cyber Security Strategy, 2008. At http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf , p. 3-5.

[32] Czosseck, et. al., 58-59.

[33] Estonian Defence Policy in 2007," Baltic Security & Defence Review 10 (2008), 262 (261-268).

[34] Prikk

[35] Madis Turr, "Press Announcement of the CCDCOE," NATO Cooperative Cyber Defence Centre of Excellence Website, 28 October 2008. At http://www.ccdcoe.org/21.html.

[36] Prikk

[37] Prikk

[38] Prikk

[39] Prikk

[40] Czosseck, et. al., 61.

[41] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53 no. 4 (2009): 1169-1170.

[42] Shackelford, 205, 251.

[43] German Government. Cyber Security Strategy for Germany. 2011. At http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 .

[44] The Dutch Government. The National Cyber Security Strategy (NCSS): Success Through Cooperation. 2011. At http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

[45] The French Government. "Defense er securite des systemes d'information: Strategie de la France" (French Strategy for Defense of Security Information Systems), 2011. At http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011.

[46] The Government of the United Kingdom. The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. November 2011. At http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy_0.pdf.

[47] United States Senate. NSPD-54/HSPD-23 and the Comprehensive National Cyber Security Initiative, 4 March 2008. At http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=11e6955c-f56f-4d15-837b-a9bd901e8419.

[48] Estonian Information System's Authority. Facts about e-Estonia. At http://www.ria.ee/27525

Appendix A: Cyber Security Policies Implemented by Estonia, 2007-2011[1]

Measure	Purpose	When Implemented
Action Plan to Fight Cyber-attacks	Improve the government's cyber emergency preparedness processes	July 2007
Revised Implementation Plan 2007-2008 of the Estonian Information Society Strategy 2013	Broadly stipulates that critical infrastructure in Estonia should be developed so that it continues to operate in "emergency situations."	September 2007
International Advocacy	Since 2007, Estonia has become more vocal in NATO, the Council of Europe, the United Nations, and other organizations, pushing for the ratification of the Budapest Cybercrime Convention and increased international cyber security.	2007-Present
Various Changes to Estonian criminal law; update of the Electronic Communications Act	Review and changes to the Estonian penal code, and amendments to relevant criminal procedure law.	2007-2010
Cyber Security Strategy	Develop a large-scale system of security measures, increase competence, improve the legal framework, bolster international cooperation, and raise cyber security awareness.	May 2008 (Implementation plan adopted in May 2009)
Cooperative Cyber Defense Center of Excellence	An Estonian-hosted international research organization whose role is set under a NATO concept. This organization researches ways to increase national and international cyber security.	2008
Cyber Security Council	Created under the Cyber Security Strategy, this Council reports directly to the Government Security Committee.	May 2009
Emergency Act	More fully incorporates cyber into the national emergency act.	June 2009
Estonian Informatics Center	State agency tasked to provide cyber security for public information services and systems. A department of Critical Information Infrastructure Protection (CIIP) was added in 2009.	2009
Cyber Defense League	Collection of information security volunteers who assist the Estonian Defense League in crisis.	2010
National Security Concept	Updated version includes additional attention to cyber security, including cyber crime and terrorism. States that the government should reduce vulnerabilities of critical systems, develop necessary legislation, and raise public awareness.	May 2010
Guidelines for Development of Criminal Policy until 2018	Police will focus on the spread of hacking and malware, and increase the number of law enforcement specialists.	October 2010

[1] Source: Czosseck, et. al.