Journal of Strategic Security

Volume 4
Number 2 *Volume 4, No. 2, Summer 2011: Strategic Security in the Cyber Age*

Article 4

Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses

Stephen Herzog
Federation of American Scientists, Washington, D.C., stephen.michael.herzog@gmail.com

pp. 49-60

Recommended Citation
Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): : 49-60.
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3
Available at: http://scholarcommons.usf.edu/jss/vol4/iss2/4

Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses

Author Biography

Stephen Herzog is a visiting research associate with the Strategic Security Program at the Federation of American Scientists. He has published reports, journal articles, and op-ed commentaries on issues such as nuclear arms control and nonproliferation, NATO strategic and contingency planning, and U.S.-China relations. Most recently, his writing has been published in the Financial Times, The Hill, and the San Francisco Chronicle, among others. He holds an M.A. in Security Studies from Georgetown University and a B.A. in International Relations from Knox College.

Abstract

In April 2007, the Estonian Government moved a memorial commemorating the Soviet liberation of the country from the Nazis to a less prominent and visible location in Tallinn. This decision triggered rioting among Russian-speaking minorities and cyber terrorism targeting Estonia's critical economic and political infrastructure. Drawing upon the Estonian cyber attacks, this article argues that globalization and the Internet have enabled transnational groups—such as the Russian diaspora—to avenge their grievances by threatening the sovereignty of nation-states in cyberspace. Sophisticated and virtually untraceable political "hacktivists" may now possess the ability to disrupt or destroy government operations, banking transactions, city power grids, and even military weapon systems. Fortunately, western countries banded together to effectively combat the Estonian cyber attacks and minimize their effects. However, this article concludes that in the age of globalization, interdependence, and digital interconnectedness, nation-states must engage in increased cooperative cyber-defense activities to counter and prevent devastating Internet attacks and their implications.

Journal of Strategic Security
Volume IV Issue 2 2011, pp. 49-60
DOI: 10.5038/1944-0472.4.2.3

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses

Stephen Herzog
Federation of American Scientists
Washington, D.C. USA
stephen.michael.herzog@gmail.com

Abstract

In April 2007, the Estonian Government moved a memorial commemorating the Soviet liberation of the country from the Nazis to a less prominent and visible location in Tallinn. This decision triggered rioting among Russian-speaking minorities and cyber terrorism targeting Estonia's critical economic and political infrastructure. Drawing upon the Estonian cyber attacks, this article argues that globalization and the Internet have enabled transnational groups—such as the Russian diaspora—to avenge their grievances by threatening the sovereignty of nation-states in cyberspace. Sophisticated and virtually untraceable political "hacktivists" may now possess the ability to disrupt or destroy government operations, banking transactions, city power grids, and even military weapon systems. Fortunately, western countries banded together to effectively combat the Estonian cyber attacks and minimize their effects. However, this article concludes that in the age of globalization, interdependence, and digital interconnectedness, nation-states must engage in increased cooperative cyber-defense activities to counter and prevent devastating Internet attacks and their implications.

Introduction

During the information age, the Internet has facilitated dramatic increases in worldwide interconnectivity and communication. This form of globalization has yielded benefits, such as improved standards of living in the developing world, but it has also given rise to new weapons of resistance for groups seeking to oppose certain political measures and ideologies. One demonstration of the latter point came about through the cyber attacks on Estonia in April and May 2007 by digital activists from the Russian diaspora. This article examines these fundamentally political attacks in cyberspace within the overall context of globalization. It argues that the situation that unfolded in Estonia in the spring of 2007 illustrates the increasing ability of transnational networks to use digital tools to challenge the policies and sovereignty of nation-states worldwide. However, the multinational responses to the Estonian cyber terrorist attacks demonstrate the growing interest of states in defending national sovereignty in the realm of cyberspace.

Ethnic Tensions in Estonia

Estonia and Russia have a long history of strife in their bilateral relationship, and the problems between these ethnic populations date back to hundreds of years before the existence of modern nation-states. Following the Soviet annexation of the Baltic States in 1940, and throughout the Cold War, the Kremlin relocated hundreds of thousands of ethnic Russians to Estonia. The purpose behind these mass migrations was two-fold: to increase cohesion in the Eastern Bloc and to "Russify" Estonian culture. Following the end of the Cold War and the dissolution of the U.S.S.R., the government in Tallinn implemented policies designed to minimize Russian influences on Estonian culture.[1, 2] And although Estonia joined NATO in 2004 and received the Atlantic Alliance's Article 5 mutual security guarantee, distrust of Moscow's intentions remains strong. After several years of lobbying, Estonia recently received NATO contingency plans to protect the country in the event of a hypothetical Russian invasion.[3] There are also reports that the government has even created house-to-house defense plans against Russian aggression.[4]

The cyber attacks on Estonia occurred within the overall climate of tension between ethnic Estonians and the country's Russian minority population. On April 30, 2007, the government moved the Bronze Soldier—a memorial commemorating the Soviet liberation of Estonia from the Nazis—from Tõnismägi Park in central Tallinn to the Tallinn Military Cemetery. This decision sparked rioting among the Russian-

http://scholarcommons.usf.edu/jss/vol4/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3

speaking community, which comprised around 26 percent of Estonia's population in 2007.[5] To ethnic Estonians, the Bronze Soldier symbolized Soviet oppression. But to Russian minorities, its relocation represented further marginalization of their ethnic identity. As Mary Kaldor and David Szakonyi argue,[6, 7] a perceived attack on the identity of a subordinate group is likely to provoke a nationalist backlash, as occurred in Estonia. In addition to rioting and violence from April 27 to May 18, distributed denial-of-service (DDoS) cyber attacks targeting the country's infrastructure shut down the websites of all government ministries, two major banks, and several political parties. At one point, hackers even disabled the parliamentary email server.[8] Estonian officials like Foreign Minister Urmas Paet quickly accused Russia of perpetrating the attacks, but European Commission and NATO technical experts were unable to find credible evidence of Kremlin participation in the DDoS strikes.[9]

Globalization and Electronic Resistance

Increased communication, networking, and reliance on digital infrastructure in the information age empower transnational resistance movements and create new vulnerabilities for nation-states. In the global Russian diaspora community, email and inexpensive international telephone services "create a shared immediacy and 'virtual' togetherness."[10] When combined with satellite television, the wide availability of Russian-language publications, and a plethora of Internet forums, these elements of globalization have enabled the Russian ethnic identity to transcend geopolitical borders. During the cyber attacks on Estonia, Russian-language forums provided news updates and a recruiting ground for interested hackers. This indicates that—in addition to a shared identity—digital technology enables rapid transnational mobilization in times of crisis.

Alongside eased mobilization across the global Russian diaspora, Estonia's dependency on information technology (IT) provided angry hackers with several appealing targets for DDoS attacks. Like most other western states, Estonia relies on the Internet for its critical infrastructure; electronic networks are integral to the functioning of government operations, electric power grids,[11] banking services, and even Tallinn's water supply. In Estonia, 97 percent of bank transactions occur online; and in 2007, 60 percent of the country's population used the Internet on a daily basis.[12] Further, Mihkel Tammet, the IT director at the Estonian Defense Ministry, explains that the Estonian state is so reliant on the Internet that its model of government operations is referred to as "paperless government."[13] The only Estonian bank to report its operating losses due to the

strikes estimated around $1 million in damages,[14] and the attacks prevented credit card and automatic teller machine transactions from occurring for several days.[15] Meanwhile, the hackers disabled the parliamentary email server and the IT capabilities of several government ministries, paralyzing the state's ability to effectively respond. During the crisis, former White House cyber-security advisor Howard Schmidt even went so far as to say, "Estonia has built their future on having a high-tech government and economy, and they've basically been brought to their knees because of these attacks."[16]

This type of transnational digital mobilization to exploit the vulnerabilities of nation-states for political purposes exemplifies the emergent threat of cyber terrorism. James Lewis of the Center for Strategic and International Studies (CSIS) offers a clear definition of this phenomenon, noting that cyber terrorism "is the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, and government operations) or to coerce or intimidate a government or civilian population."[17] In the case of Estonia, the cyber-terrorist attacks occurred through the use of globally dispersed and virtually unattributable botnets of "zombie" computers. The hackers hijacked computers—including many home PCs—in places like Egypt, Russia, and the United States and used them in a "swarming" DDoS strategy. Government and bank websites that normally received 1,000 visits a day crashed after receiving upwards of 2,000 hits a second.[18] Estonian authorities made a few in-country arrests but never uncovered the main culprits, who were allegedly operating out of Russia.

While the cyber-terror attacks on Estonia shocked the international community, by most accounts, they could have been significantly more devastating. In future assaults, hackers may target a state's traffic lights, water supply, power grids, air traffic controls, or even its military weapon systems. As the Estonian crisis indicates, the Internet has become a powerful asymmetric tool for transnational groups who view themselves as disenfranchised and seek to intimidate the nation-states and other actors presumably responsible for their grievances. This is an issue of national sovereignty, as the digital networks and critical infrastructure targeted by the hackers are the property of—or on the territory of—nation-states.

Interstate or Transnational Threat?

Scholars, practitioners, and students of international security are well aware of the development of advanced cyber-warfare capabilities by states around the world like China, Israel, Russia, and the United States. The

http://scholarcommons.usf.edu/jss/vol4/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3

rise of these capabilities and their attendant strategies has led many countries to include cyber attacks as an area of concern in their national security doctrines. For instance, Washington lists violence in cyberspace as a threat alongside traditional terrorism, the proliferation of weapons of mass destruction, and transnational crime in its National Security Strategy.[19] Nonetheless, Douglas Thomas of the University of Southern California contends that "99 percent of…hackers do not have the skill or the ability to organize or execute an attack that would be anything more than a minor inconvenience."[20] Given Russia's advanced cyber-war capabilities and the gravity of the attacks on Estonia, it is a legitimate question to ask if the attacks were truly executed by autonomous networks of Russian-speaking hackers or if they were committed or sponsored by the Kremlin.

Even though EU and NATO technical experts were unable to find evidence of Russian involvement in the Estonian cyber-terror incident, it certainly would have been in Moscow's interests to organize DDoS strikes. After the movement of the Bronze Soldier and clashes between police and demonstrators, Russian officials accused Tallinn of human rights violations and demanded that Prime Minister Andrus Ansip apologize and resign from office.[21] While Russia categorically denied any involvement in the attacks, one unnamed NATO official did not mince words: "I won't point fingers. But these were not things done by a few individuals. This clearly bore the hallmarks of something concerted."[22] Because of economic interdependence and the threat of nuclear escalation, Russia cannot risk attacks on NATO member states,[23] perhaps making unattributable cyber strikes an attractive alternative. In addition to the fact that NATO's conventional military forces significantly outnumber those of the Russian Federation,[24] Estonia serves as a key transit country for Russian oil and natural gas supplies to Central and Western Europe. And for all the rhetoric about Russia's coercive energy politics, Moscow exports over 90 percent of its gas and oil to Europe,[25] fostering a situation of mutual economic interdependence. A conventional Russian attack on Estonia would trigger a NATO Article 5 response and could compromise the energy wealth that has led to growing Russian influence on the international stage. In a world of deterrence and interdependence, virtually untraceable digital displays of force could allow states to subvert the constraints of the international system.

While we may never know the true extent of Kremlin involvement in the cyber attacks on Estonia, it is clear that Russian officials encouraged the hackers by accusing Tallinn of altering history, perpetrating human rights violations, and encouraging fascism.[26] The Russian authorities also turned a blind eye as pro-Kremlin activists blockaded the Estonian

embassy in Moscow for several days.[27] Although it would have served Russian national interests to test Moscow's cyber-war capabilities on Estonia, the general consensus among experts is that sophisticated "hacktivists" in Russia—and possibly throughout the global Russian diaspora—perpetrated the attacks.[28] The alarming reality of the situation is that, in the information age, computer-savvy individuals can now threaten the sovereignty and wellbeing of nation-states, oftentimes from the comfort of their own homes.

Multinational Responses to Cyber Terror

The 2007 cyber terrorism on Estonia was more than just a temporary nuisance; rather, it was a mild version of a new form of digital violence that could halt public services, commerce, and government operations. Estonian Defense Minister Jaak Aaviksoo observed that successful cyber attacks "can effectively be compared to when your ports are shut to the sea."[29] A blockade is a fitting analogy, as future cyber-terrorist attacks may disrupt a country's water and electricity supplies, telecommunications (severing its connections to the world), and national defenses.

The seriousness of the attacks on Estonia generated a rapid international response. Estonia had few formal cyber-defense preparations outside of its framework for countering traditional acts of terrorism,[30] and the government Computer Emergency Response Team (CERT) required Finnish, German, Israeli, and Slovenian assistance to restore normal network operations.[31] NATO CERTs provided additional assistance, while the EU's European Network and Information Security Agency (ENISA) offered expert technical assessments of the developing situation. Further, a high level of intelligence sharing took place among western countries during the crisis. While Russian-speaking hackers employed the Internet as a weapon and tool of mobilization, Estonia and its allies used digital networks to successfully counter the attacks.

During and after the DDoS strikes, NATO and EU member states began to debate new directions for cyber security and the appropriate punishments for states found to have engaged in digital warfare. Sanctions were one punishment option that received fairly widespread support. Additionally, one German official even recommended that NATO consider extending its Article 5 security guarantees to the realm of cyberspace.[32] At its Bucharest Summit in April 2008, NATO adopted a unified Policy on Cyber Defence and created the Brussels-based Cyber Defence Management Authority (CDMA) to "centralise cyber defence operational capabilities across the Alliance."[33] And in August 2008, Tallinn became home to the

http://scholarcommons.usf.edu/jss/vol4/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3

NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), the Atlantic Alliance's cyber-security headquarters. On the EU front, in November 2010, the organization released its Internal Security Strategy, which calls for integrated responses to cyber-security threats and significant expansion of ENISA's duties beyond its previously limited analytical role.[34]

Beyond these efforts, throughout 2010 and in the early months of 2011, both organizations announced a series of concrete long-term plans aimed at countering cyber attacks. The EU's new Digital Agenda for Europe revealed plans to establish CERTs for EU institutions, hold multinational cyber-defense simulations, and create a joint European cyber-crime platform.[35] NATO adopted a new Strategic Concept in Lisbon in November 2011, which indicated that the alliance will take steps to develop strong, integrated Internet defense capabilities.[36] To that end, General Stéphane Abrial, head of NATO's Allied Command Transformation, has confirmed that the NATO Computer Incident Response Capability Technical Centre (NCIRC TC) in Mons, Belgium will become operational in 2012.[37] These EU and NATO actions are indicative of the growing recognition of the severity of today's digital threats. As U.S. Deputy Secretary of Defense William Lynn warned when discussing NATO vulnerabilities in light of the Estonian case, "The potential exists for capabilities that are much more destructive…We're largely in the exploitation/denial phase, but history will tell you that somebody will take it to the extreme."[38]

The multinational responses to the 2007 attacks on Estonia indicated that countries would not remain detached and complacent as states or non-state actors threatened the sovereignty of their allies by using the Internet as a weapon. Still, it is important to note that the international response to the events in Estonia occurred within the confines of preexisting security communities. Russia tolerated and encouraged the cyber attacks, and the Kremlin may have even colluded with the hackers responsible for the strikes. China addressed the matter as an internal Estonian security dilemma and eschewed involvement in the resultant international cyber-security discussions. Regardless of any secret complicity or participation in the Estonian cyber attacks, Moscow and Beijing surely analyzed the situation, assessed Tallinn's vulnerabilities and western responses, and improved upon their own cyber-warfare capabilities and strategies as a result.

Conclusion

The severity of the Estonian cyber attacks served as a wake-up call to the world, as it became clear that potentially autonomous transnational networks—like unhappy pro-Kremlin "hacktivists"—could avenge their grievances by digitally targeting and nearly crippling the critical infrastructure of technically sophisticated nation-states. In the future, an enhanced focus on cyber security and new multinational strategies and institutions will be instrumental in countering electronic threats to the sovereignty and survival of states. However, the world of information security is not unlike the traditional global security environment; for each visible action, there is oftentimes a commensurate reaction. The attacks on Estonia will likely encourage future groups of transnational imitators, and the events of spring 2007 have provided states with important information for the further development and improvement of their own cyber-warfare capabilities.

The benefits of the information age are numerous, but nascent threats like transnational cyber terrorism and information warfare exist alongside the positive aspects of globalization. In this period of IT-driven globalization, the attacks on Estonia demonstrate that even NATO Article 5 and U.S. nuclear umbrella guarantees cannot ensure the protection of a nation-state's sovereignty in cyberspace. A new challenge has emerged for free societies: democracies must find ways to strike a balance between allowing Internet freedom on one hand and maintaining adequate early warning and monitoring systems on the other. These systems, combined with expanded cyber-security cooperation across borders, will be integral in detecting suspicious digital activities and countering attempted acts of cyber warfare and cyber terrorism. Just as the world economy has adapted to the digital era, the Estonian cyber terrorism case indicates that the foreign and security policies of nation-states must also do so, as difficult-to-attribute asymmetric threats stemming from the Internet are likely to harm nation-states in the future.

About the Author

Stephen Herzog is a visiting research associate with the Strategic Security Program at the Federation of American Scientists. He has published reports, journal articles, and op-ed commentaries on issues such as nuclear arms control and nonproliferation, NATO strategic and contingency planning, and U.S.-China relations. Most recently, his writing has been published in the *Financial Times*, *The Hill*, and the *San Francisco Chronicle*, among others. He holds an M.A. in Security Studies from

http://scholarcommons.usf.edu/jss/vol4/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3

Georgetown University and a B.A. in International Relations from Knox College. He may be reached for comment at *stephen.michael.herzog@gmail.com*. The views expressed in this article are his own.

References

1 Examples of these policies included the implementation of Estonian language fluency tests prior to receiving citizenship and public school diplomas. See: David J. Smith, "Minority Rights, Multiculturalism and EU Enlargement: The Case of Estonia," *Journal on Ethnopolitics and Minority Rights Issues in Europe* 4:1 (2003): 1, 22. 23. However, it should be noted that Estonia has since revised many of these policies and now exceeds the minority rights standards set forth for the country by the Organization for Security and Cooperation in Europe.

2 For a discussion of Russian minority rights and integration challenges in Estonia see Marju Lauristin and Mati Heidmets (eds.), *The Challenge of the Russian Minority: Emerging Multicultural Democracy in Estonia* (Tartu: Tartu University Press, 2002).

3 "Contingency Plans for Baltic Countries Actually In-The-Works—Lithuania's Grybauskaite," Baltic News Service, June 15, 2010, accessed through LexisNexis. See also: "NATO and Russia: Trust, but make military plans," *The Economist*, July 29, 2010, accessed through LexisNexis.

4 Gundar J. King and David E. McNabb, "Crossroads Dynamics in Foreign Policy: The Case of Latvia," *Problems of Post-Communism* 56:3 (June 2009): 35.

5 Statistics Estonia (government census bureau), "Population by ethnic nationality, 1 January, year," Tallinn, updated October 13, 2010, available at: *http://www.stat.ee/34278*.

6 See Mary Kaldor, "Nationalism and Globalisation," *Nations and Nationalism* 10:1–2 (2004): 161–177.

7 See David Szakonyi, "The Rise of Nationalism under Globalization and the Case of Post-Communist Russia," *Vestnik: The Journal of Russian and Asian Studies* 6 (Summer 2007), available at: *http://www.sras.org/economic_nationalism_under_globalization*.

8 Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9:1 (Winter/Spring 2008): Columbia International Affairs Online.

9 "Estonia has no evidence of Kremlin involvement in cyber attacks," RIA Novosti, September 6, 2007, available at: *http://en.rian.ru/world/20070906/76959190.html*.

10 Jürgen Osterhammel and Niels P. Petersson, *Globalization: A Short History*, trans. Dona Geyer (Princeton: Princeton University Press, 2005), 8.

11 In an interview, James Lewis of the Center for Strategic and International Studies provided several reasons why power grids would make appealing cyber-terror targets. Lewis explained that city power generators used in the United States "require a lead time of three or four months to order them." It is likely that replacing power generators in other countries would also require significant lead time. [James A. Lewis, interview by Steve Croft, *60 Minutes*, CBS, Washington, November 8, 2009), available at: *http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml*.]

12 Ruus, 2008.

13 Quoted in "The cyber raiders hitting Estonia," *BBC News*, May 17, 2007, available at: *http://news.bbc.co.uk/2/hi/europe/6665195.stm*.

14 Marcin Terlikowski, "Cyber attacks on Estonia. Implications for International and Polish Security," *Polish Quarterly of International Affairs* 16:3 (2007): 75.

15 Gadi Evron and Hillar Aarelaid, "Estonia: Information Warfare and Lessons Learned" (presentation, *European Commission* Workshop on Learning from Large Scale Attacks on the Internet—Policy Implications, Brussels), January 17, 2008, available at: *http://tinyurl.com/ycslpvq (ec.europa.eu/information_society/policy/nis/docs/largescaleattacksdocs/s5_gadi_evron.pdf)*. Given the consequences for the Estonian economy, one can only imagine the economic losses that might result from widespread cyber attacks across the EU, for example. The EU's economy accounts for over $16 trillion annually; 81 percent of businesses rely on broadband Internet, and 75 percent of EU citizens use the Internet daily. Due to EU interconnectedness, a well-executed campaign of cyber terrorism on one state could trigger a ripple effect costing billions of dollars in economic damages. Meanwhile, strikes on government networks could slow or hinder the ability of countries to respond. See: "Europe's Digital Competitiveness Report 2009," European Commission, August 4, 2009, available at: *http://tinyurl.com/l9yb6j (ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2009/sec_2009_1103.pdf)*.

16 Quoted in Larry Greenemeier, "Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter,'" *Information Week*, 24 (May 2007).

17 Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats," Center for Strategic and International Studies, Washington, December 2002, 1, available at: *http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf*.

18 Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Washington: Congressional Research Service, 2007), 7.

19 White House, *National Security Strategy*, May 2010, 27–28, available at: *http://tinyurl.com/38wx76w (www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf)*.

20 Quoted in Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" *USIP Special Report* (Washington, United States Institute of Peace, May 2004): 9.

21 Terlikowski, 2007, 71.

http://scholarcommons.usf.edu/jss/vol4/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3

22 Quoted in Myriam Dunn Cavelty, "Critical information infrastructure: vulnerabilities, threats, and responses," *Disarmament Forum* 9:3 (2007): 15. Some IP addresses used by the hackers were traced to Russian government computers, but it is possible that the cyber terrorists penetrated Kremlin networks in order to confuse international investigators. [Ruus, 2008.]

23 See, for example, Robert O. Keohane and Joseph S. Nye, "Power and Interdependence Revisited," *International Organization* 41:4 (Autumn 1987): 727–733, 737–740.

24 Russia has around one million active-duty troops. NATO maintains over two million forces in Europe, and its aggregate forces account for over three million troops. See: International Institute for Strategic Studies, *Military Balance 2010* (London: Routledge, 2010), 28–52, 119–173, 222.

25 Angela Stent, "An Energy Superpower? Russia and Europe," in Kurt M. Campbell and Jonathon Price (eds.), *The Global Politics of Energy* (Washington: Aspen Institute, 2008), 78.

26 Terlikowski, 2007, 71. While there is no conclusive evidence of the Russian government assisting the hackers, the Kremlin also appeared to support the attacks by suspending some of its trade with Estonia and refusing to cooperate in Tallinn's investigation of the strikes. See: Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4:3 (Fall 2010): 110.

27 Ruus, 2008.

28 There is still some debate on this issue. Given the small size of Estonia and its digital infrastructure, many analysts believe that groups of hackers around the world could have perpetrated the strikes. Even Hillar Aarelaid, head of Estonia's CERT, "expressed skepticism that the attacks were from the Russian government." See: Bill Brenner, "Experts doubt Russian government launched DDoS strikes," Security Wire Daily News, May 18, 2007, available at: *http://tinyurl.com/3ofppqg (searchsecurity.techtarget.com/news/1255548/Experts-doubt-Russian-government-launched-DDoS-attacks)*.

29 Quoted in Ruus, 2008.

30 For a discussion of Estonia's previous framework for countering traditional terrorism and cyber terrorism, see Ulrich Sieber and Phillip W. Brunst, *Cyberterrorism—the use of the Internet for terrorist purposes* (Strasbourg: Council of Europe Publishing, 2007), 161–166. Following the attacks, Estonia became one of the first countries in the world to develop a comprehensive national cyber-security strategy. See: "Cyber Security Strategy," *Estonian Ministry of Defense*, 2008, available at: *http://tinyurl.com/5ruln4o (www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf)*.

31 Ruus, 2008.

32 Lewis, "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict," *Center for Strategic and International Studies*, Washington, October 2009, 3 (n-3), available at: *http://tinyurl.com/yjzvlge (csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf)*.

33 Rex B. Hughes, "NATO and Cyber Defence: Mission Accomplished?" *Netherlands Atlantic Association*, Amsterdam, *Atlantisch Perspectief* 8 (2008): 1, available at: *http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf*.

34 "The EU Internal Security Strategy in Action: Five steps toward a more secure Europe," *European Commission*, November 22, 2010, available at: *http://tinyurl.com/2cfnqg5 (ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf)*.

35 Ibid., "A Digital Agenda for Europe," May 19, 2010, 17–18, available at: *http://tinyurl.com/2dyjfvn (ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf)*.

36 "Strategic Concept For the Defence and Security of the North Atlantic Treaty Organization," *North Atlantic Treaty Organization (NATO)*, November 19, 2010, available at: *http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf*.

37 Stéphane Abrial, "NATO Builds Its Cyberdefenses," *International Herald Tribune*, February 28, 2011, available through LexisNexis.

38 Quoted in Jim Garamone, "Lynn: NATO Must Get Ahead of Cyber Threat," *American Forces Press Service*, January 25, 2011, available at: *http://www.defense.gov//news/newsarticle.aspx?id=62572*.

http://scholarcommons.usf.edu/jss/vol4/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3