Journal of Strategic Security

Volume 7
Number 1 *Volume 7, No. 1: Spring 2014*

Article 7

International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic

Nadiya Kostyuk
EastWest Institute, nadiya@umich.edu

pp. 68-82

Recommended Citation
Kostyuk, Nadiya. "International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic." *Journal of Strategic Security* 7, no. 1 (2013): : 68-82.
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6
Available at: http://scholarcommons.usf.edu/jss/vol7/iss1/7

International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic

Author Biography

Nadiya Kostyuk is a Program Coordinator for the Worldwide Cybersecurity Initiative at the EastWest Institute.Prior to joining the institute, Nadiya interned at the United Nations Population Fund (UNFPA), the International Coalition for the Responsibility to Protect (ICRtoP) and the Neighborhood Defender Service of Harlem. She spent the past two years conducting interviews with government officials, academics and journalists, researching policy gaps in the current European cybersecurity paradigm. In-country experience in Bosnia and Herzegovina, Estonia, Ukraine, Russia, Serbia, Sweden, Switzerland and the Czech Republic provided her with a better understanding of each country's unique political climate. This summer, Nadiya participated in the NATO Summer School, where she joined in interactive workshops and simulations with international security experts, discussing best cybersecurity practices. Nadiya holds a master's degree in Global Affairs, with a concentration in Transnational Security (Cybersecurity) from New York University. In addition to her native Ukrainian, Nadiya is fluent in Russian and proficient in German.

Abstract

While many countries and companies have fallen victim to cyber attacks over the past few years, including American companies such as Apple, Microsoft, and Facebook, Czech websites remained relatively safe until March 2013, when they were interrupted by a series of cyber attacks. Even though the origin of the attacks remains debatable, this case study demonstrates the importance of cooperation between nations in the nascent phase of the internet development and their more powerful allies. Domestic challenges that nations face in addressing cybersecurity in an effective and comprehensive manner include ambiguous legislation, recalcitrant officials, and a lack of both fiscal and human capital. To address these challenges, nations should cooperate with their more capable allies, such as the EU and NATO, create better cyber protective measures, train and hire qualified specialists in the public sector, and intensify private-public partnership. Until an international agenda on cyberspace is set, these nations with limited resources should cooperate with developed nations lest they risk more severe attacks in the future.

Introduction

"The nature of the technology is the root cause of the incentive system that encourages states to attack each other in cyberspace: attribution is difficult; cyber weapons easily cross borders; both civilian and government victims are reluctant to admit they have been attacked or penetrated…[T]he offense has distinct advantages over the defense; and the norms that determine thresholds for retaliation for non-cyber attacks do not apply well to attacks from cyberspace."

- Richard Andres[1]

While many countries and companies have been victims of cyber attacks over the past few years, including American companies Apple, Microsoft, and Facebook, Czech websites remained relatively safe until March 2013.[2] Specifically, from March 4-7, 2013, cyber attacks disabled the online media outlets of *Hospodářské noviny* (iHned.cz) and *Mladá fronta Dnes* (iDnes.cz).[3] On March 4th, the attacks targeted the largest and the most visited news servers and came in two waves: in the morning from 9 AM to 11 AM (local time), and in the afternoon from 2 PM to 4 PM.[4] Monday morning attacks targeted new servers: www.novinky.cz, www.iHNed.cz, www.Lidovky.cz, www.Denik.cz, www.iDNES.cz; and, in the afternoon, www.E15.cz, www.Zive.cz, www.Mobilmania.cz were under attack. The most popular Czech search engine, Sezman.cz, and the Prague Stock Exchange were affected by denial-of-service (DoS) attacks on March 5.[5] The attack occurred from 10 AM to 11:30 AM and reoccurred at 1:30 PM causing unavailability of the search engine. The servers of the Czech National Bank and several other commercial banks including Ceska sporitelna, Komercni banka, and Raiffeisenbank were blocked with hundreds of thousands of requests on March 6th.[6] These cyber attacks also came in two waves: from 9.30 AM to 11 AM and at 2 PM. The 6th and 7th of March also saw attacks on CSOB, the Czech Republic's largest bank, and two national mobile phone operators whose online services were disabled from attacks that bank officials claimed "[came] from abroad."[7] On

[1] Richard Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in Derek Reveron (ed.), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, D.C.: Georgetown University Press, 2012), 100.
[2] Agence France-Presse, "Hackers attack top Czech news websites," *Raw Story*, March 4, 2013, available at: *http://www.rawstory.com/rs/2013/03/04/hackers-attack-top-czech-news-websites/.*
[3] Jeffrey Goldman, "Leading Czech News Sites Hit by Cyber Attacks," *eSecurity Planet*, March 5, 2013, available at: *http://www.esecurityplanet.com/network-security/leading-czech-news-sites-hit-by-cyber-attacks.html.*
[4] Narodni Centrum Kyberneticke Bezpecnosti. Denial of Service attacks in the Czech Republic in March 2013.
[5] Denial-of-service (DoS) attacks "targets networks, systems and individual services, and flood them with so much traffic that they either crash or are unable to operate – which effectively denies the service to legitimate users," as it is defined at: Check Point Software Technologies LTD, *Check Point 2013 Security Report*, January 2013; Andrew Greene, "Officials react to cyber attacks," *Prague Post,* March 13, 2013, available at: *http://www.praguepost.com/news/15698-officials-react-to-cyber-attacks.html.*
[6] Erik Nelson, Richard Parrish, and Connor Zickgraf, "New Group Launches Czech Cyber Attack, Interim Bulgarian Government Takes Helm," *Transitions Online: Regional Intelligence*, March 14, 2013, available at: *http://www.tol.org/client/article/23658-new-group-launches-czech-cyber-attack-interim-bulgarian-government-takes-helm.html.*
[7] "UPDATE 2-Czech central bank, stock exchange, banks' sites hacked," *Reuters*, March 6, 2013, available at: *http://www.reuters.com/article/2013/03/06/czech-hackers-banks-idUSL6N0BY52420130306.*

March 11th, a new series of more sophisticated attacks—distributed denial-of-service (DDoS) attacks—began, halting the work of the Czech bank UniCredit.[8]

Oldrich Krulik of the Czech Republic Police Academy and Tomas Rezek with the Association for International Affairs (AMO) agree that although the Czech Republic is technologically well-connected, it lacks a proper cyber *shield* (defensive capabilities) and thus is a perfect target for hackers who want to test their capabilities in preparation for a future cyber attack on a country that may have more sophisticated cyber protective measures.[9] Assuming that Krulik and Rezek are correct, there are some natural concerns, including how long this practice can last and what the next target will be. Having conducted semi-structured interviews with representatives from academia and the press, and with Czech and Russian cyber professionals from the private and public sectors, this research will address the difficulties of attack origin-attribution in cyber space and subsequent target prediction, and will provide future policy recommendations to help reduce the number of cyber intrusions in the Czech Republic and similarly-positioned states. Since the national security authority *Narodni bezpecnostni urad* (NBU) is currently working on drafting and implementing cyber security legislation, these research findings are especially significant and timely for the Czech Republic.

Assessing the Damage

The attacks that occurred in the Republic were SYN floods, low-level attacks that target capacity of servers to accept new connections, causing some services to go offline.[10] The affected companies' losses were minimal as no data was stolen or compromised. Ondrej Filip, the CEO of CZ. NIC that deals with cybersecurity, supports this conclusion by mentioning that online banking was disabled for some banks but the damage could not be measured in monetary terms as the attacks did not cause any real impact.[11] The consultancy firm PriceWaterhouseCoopers, however, concluded that the recent attacks cost Czech Web servers, media, and banks less than 10 million Kč (about $507,800 USD) while the corporate internal costs associated with the fight against cyber perpetrators are lower than 1 million Kč ($50,700 USD).[12] Furthermore, Rezek does not view the DDoS attacks as very destructive since "the usage of online banking and potential dependency on this service is rather low in the Czech Republic, therefore the unavailability of this service was rather a nuisance than significant problem."[13] Rezek continues that the attacks in the Republic were not strong enough to bring down any important infrastructure and were not aimed against any Internet providers.[14]

---

[8] Distributed Denial-of-service (DDoS) attack is "coordinated and simultaneously launched from multiple sources to overwhelm and disable a target service," as it is defined at *Check Point 2013 Security Report*, see note 5 above; Nelson, see note 7 above.
[9] Oldrich Krulik, Personal Interview, March 18, 2013; Tomas Rezek, Personal Interview, March 17, 2013.
[10] A SYN flood attacks is a form of denial-of service attacks when an attacker sends numerous SYN requests to a server with a purpose of overwhelming it with requests to make the system unresponsive to legitimate traffic. Martin Koldovsky, E-mail Interview, April 2, 2013.
[11] Masha Volynsky, "Cyber attacks taunt experts and raise security concerns," *Radio Prague,* March 12, 2013, available at: *http://www.radio.cz/en/section/curraffrs/cyber-attacks-taunt-experts-and-raise-security-concerns.*
[12] Greene, see note 6.
[13] Thomas Rezek, E-mail Interview, March 31, 2013.
[14] Ibid.

http://scholarcommons.usf.edu/jss/vol7/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6

Czech Republic Cyberspace

Similar to many other developed and developing European nations, the Czech Republic can be called "a primitive cyber society" as the integration of the Internet into commercial, government, and interpersonal transactions and subsequent Internet infiltration into all areas of Czech life are relatively recent.[15] Cybersecurity became an issue of Czech national security in 2001 when the number of Internet users increased significantly. In 2011, more than 60 percent of Czech residents owned PCs and more than 50 percent had Internet connection, compared to the U.S. with 75.6 percent and 71.7 percent, respectively.[16] The percentage of the population with Internet connection in the country is predicted to rise to 75 percent by 2016.[17] Moreover, a government tax rebate on computer purchases will most likely keep the consumer PC market in the country growing.[18] This drastic increase in the number of Internet users has given rise to over eight hundred Internet providers, the leading companies being Telefonica, T-Mobile, and UPC.[19] Following the recent increase in cyber attacks worldwide, especially on governmental databases, Czech governmental bodies have been implementing basic levels of protection. Ninety-nine percent of government offices, for instance, have virus-detection programs, 88 percent of them have installed hardware or software firewalls, 98.1 percent have regular data backups, and 97.9 percent use electronic signatures.[20] Moreover, cybersecurity standards have notably improved among private companies that have foreign owners and there is also easy access to information regarding the best practices in the field of cyber protection. As shown by the March 2013 attacks, however, these changes are hardly enough. The only publicly available information regarding governmental initiatives is that the drafting process of the cyber legislature is ongoing. With many individuals, businesses, and agencies connected to the Internet and lacking proper cyber security measures, the Czech Republic remains a soft target for an online attack.[21]

Czech Cybersecurity Strategy: Domestic Challenges

Even though the Czech Republic 2011-2015 Cyber Security Strategy was adopted, "mark[ing] the beginning of an active national cyber-defense policy," it only set up a theoretical blueprint for cybersecurity as the actual implementation of this strategy has been delayed significantly due

[15] Will Goodman, "Cyber Deterrence Tougher in Theory than in Practice?" *Strategic Studies Quarterly* (2010): 110.
[16] "Use of PC in Household and Individuals in 2011," Czech Statistical Office, available at: http://www.czso.cz/csu/2011edicniplan.nsf/engkapitola/9701-11-eng_r_2011-0302; "Use of PC in Household and Individuals in 2011," Czech Statistical Office, available at: *http://www.czso.cz/csu/2011edicniplan.nsf/engkapitola/9701-11-eng_r_2011-0302;* Thom File, "Computer and Internet Use in the United States," available at: *http://www.census.gov/prod/2013pubs/p20-569.pdf.*
[17] Czech Statistical Office, see note 18.
[18] "Russia Information Technology Report Q1 2013," *Business Monitor International* 16, February 6, 2013, available at: *http://www.marketresearch.com/Business-Monitor-International-v304/Russia-Information-Technology-Q1-7350837/.*
[19] The total number of Internet providers presented on the webpages of http://rychlost.cz/isp/ [access: 04.01.2013].
[20] Tomas Rezek, "Cyber Security in the Czech Republic," Trans. Array *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations* (Krakow, Poland: The Kosciuszko Institute, 2012), 34.
[21] At the time of these interviews, some companies lack the basic levels of protection, mentioned earlier; Yu Chin Cheng, Internet Chat interview, April 5, 2013.

to bureaucratic malaise, including ambiguous legislation and recalcitrant officials.[22] In addition, despite the fact that the NBU is currently working on creating new cybersecurity policies with the goal of implementing them in the fall of 2014, the upcoming Czech parliamentary elections will most likely slow down the process.[23] Even though most Czech experts agree that this legislation is a stepping-stone in improving Czech cybersecurity, they may be too optimistic on the role of this new document as the legislation lacks clear definitions of cyber-related terms, which could cause divisive debate among cyber specialists. Additionally, the legislation only provides general recommendations that were mostly copied from EU documents. Rezek and Flidr agree that this new document will be compliant with the EU draft that is being finalized, reflecting about ninety percent of it, but its provisions still remain vague.[24]

Another challenge in the Czech cybersecurity agenda is that the NBU's role is still only on paper. It will take years for the NBU to be on the same level as competing private companies such as Czech Republic's national research education network CESNET and the policy making organization CZ.NIC, which have their own experts and resources to deal with cyber issues.[25] Though the Republic should not all together exclude private companies from the cybersecurity profile, it is important for the Czech government to develop in-house cybersecurity capabilities. As private companies tend to be more proactive, a joint public-private security environment will offer the best of both worlds. In addition to the NBU's weak role, most interviewees agreed that numerous agencies from public and private sectors, as well as experts from academia, do not always cooperate with each other due to various reasons, such as privacy.[26] This situation creates perfect conditions in the country that allow motivated hackers near impunity in their illegal cyber activities. Though it is still early in terms of the Czech Republic's adoption of Internet banking, potential saturation in this market combined with inadequate cybersecurity protection measures could be a catastrophic occurrence in the future.

Other recent global cyber attacks

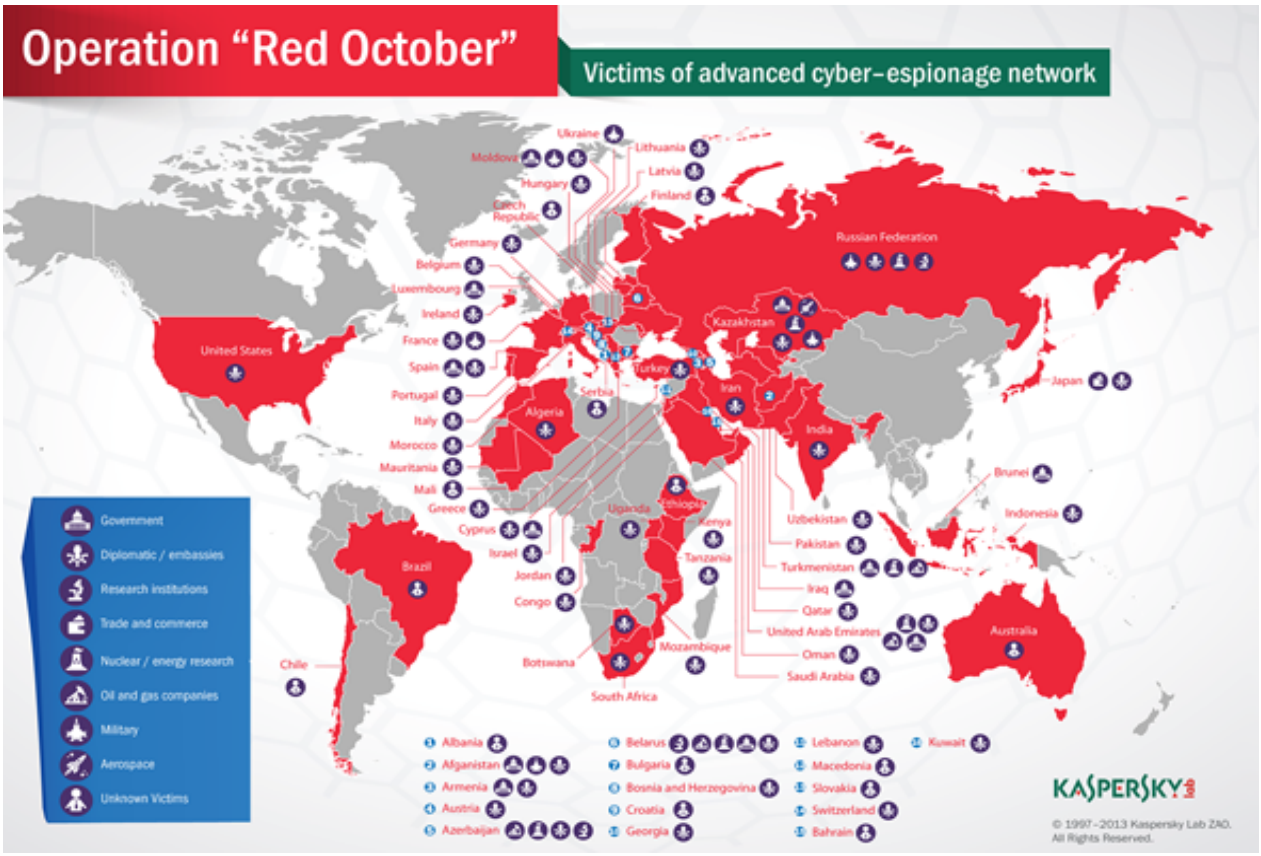
The Czech Republic is not unique in facing domestic bureaucratic challenges in policing its cyberspace. Many countries in Central and Eastern Europe, Central Asia and Africa experience a similar set of challenges since cybersecurity is, at best, new on their domestic agendas. In the early 2000s, the *ILOVEYOU* virus, which was developed by a Filipino student, caused approximately $10 million dollars in losses across twenty countries, while the so-called Nigerian 419 scams demonstrate the relative ease which motivated offenders in any nation can defraud unsuspecting persons.[27] Moreover, Operation Red October, an advanced, malware-driven

[22] "Cyber Security Strategy of the Czech Republic for the 2011 – 2015 Period," *European Network and Information Security Agency*, available at: *http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF* ; Joanna Świątkowska," Cyberthreats as a Challenge to the Security of the Contemporary World," Trans. Array *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations* (Krakow, Poland: The Kosciuszko Institute, 2012), 8.
[23] Thomas Flidr, Personal Interview, June 26, 2013.
[24] Ibid; Tomas Rezek, E-mail l Interview, April 1, 2013
[25] Krulik, *see* note 11.
[26] Ibid; Vlastimil Cerveny, Personal Interview, March 20, 2013; Rezek, see note 11.
[27] "ILOVEYOU" Virus: Lessons Learned Report," *Assured Information for America's Power Projection Army, Department of the Army*, June 25, 2003, available at: *http://www.dtic.mil/cgibin/GetTRDoc?AD=ADA415104&Location=U2&doc=GetTR Doc.pdf* ; In the Nigerian scams, the "scammers offer victims

http://scholarcommons.usf.edu/jss/vol7/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6

espionage network that existed from October 2007 until the beginning of January 2013, involved the creation of more than sixty domains that worked as attack proxies from Russia and Germany.[28] The map below from antivirus corporation Kaspersky Lab shows the extent of the damage of Operation Red October.

Figure 1: Operation "Red October"[29]



Moreover, other developing countries all over the world are in the process of forming governing bodies responsible for developing domestic cybersecurity legislation.[30] Often these countries are inadvertent soft targets to cyber attacks due to an unclear division of responsibilities between various domestic agencies and a prevailing role of private companies in this new sector as private firms tend to possess more resources, compensate talent better than the government and

---

everything from false job promises and inheritance traps to company shares in the public and private sector, all of which cost the victim a nominal fee as a means to receive a greater prize. After a victim supplies the perpetrator with personal information, such as bank account numbers, illegal money transfers occur through companies like Western Union. The Nigerian scam has spread to other countries that have no legal base for this crime, including Togo and Cote d'Ivoire." Nadiya Kostyuk and Marielle Ali, "The Digital Front: Preemptive Approaches to Cyberwarfare," *Partnership for Research in International Affairs and Development* 2 (July 2013).

[28] Steve Gutterman. "Russia beefs up Internet security after spy attacks," *MSN News*, January 21, 2013, available at: *http://news.msn.com/science-technology/russia-beefs-up-internet-security-after-spy-attacks.*

[29] "The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies," *Securelist, Kaspersky lab expert*, January 14, 2013, available at*: http://www.securelist.com/en/blog/785/.*

[30] By using the term "developing countries," the author implies "internet developing countries."

have superior technical capabilities. For example, in the "Strategy of Development of the National Security System of the Republic of Poland 2011-2022," the private sector is responsible for securing cybersecurity.[31] Similar to the Czech Republic, Poland has the "Governmental Program for the Protection of Cyberspace in Poland for 2011-2016" ("the Program") that includes numerous useful recommendations that have not been implemented since its publication.[32] Moreover, it is not clear who or what agency is responsible for its implementation. Lastly, numerous entities are partially involved in cybersecurity, such as the Ministry of Administration and Digitalization, the Ministry of Interior, and the Internal Security Agency.[33] Because of such bureaucratic complexities, Poland is completely unprepared for cyber attacks according to a 2012 McAfee report.[34] It is apparent that Polish non-governmental entities have a better understanding of the importance of protecting cyberspace. Such a lack of initiative or agency to move swiftly on cyber security policy can be seen in Slovakia as well. Even though the preliminary design for the Act on Information Security of Slovakia was approved in February 2010, it is still unknown when the text of this act will be published and prepared for discussion.[35] Similar to the Czech "Cyber Security Strategy," the Slovak "National Strategy on Information Security" involves main points that must be clarified. The key players, however, are not clarified.

Deciphering the Czech Cyber Attacks: Attribution and Legacy

The first reaction to the cyber attacks in Czech society was to blame Russia. The Czech population still remembers the Soviet occupation of the Republic, specifically the 1948 establishment of the communist regime, the 1968 Prague Spring and the Soviet intrusion into Czech territory. As the Soviet successor, Russia has been utilizing various means, such as bribery, land acquisition, financial flow, infiltration, espionage, and the Orthodox Church, to impede the Republic's further integration and cooperation with the West.[36] Furthermore, Russia has also been linked to cyber attacks in former Soviet states, specifically Estonia and Georgia. In 2007, a cyber incident occurred in Estonia when a nineteen-year old connected to the Russian security service was accused of disabling "the websites of government ministries, political parties, newspapers, banks, and companies," but in fact, "the Kremlin may have even colluded with the hackers responsible for the strikes."[37] In 2008, a cyber case in Georgia accused Russia of disabling several Georgian websites, including the Ministry of Foreign Affairs homepage.[38]

---

[31] Ministry of Defence, Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP 2012-2022. Projekt.
[32] Światkowska, see note 27, 42.
[33] The list of other entities could be found on page 25 of "Array *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations* (Krakow, Poland: The Kosciuszko Institute, 2012), 25.
[34] Światkowska, see note 26, 49.
[35] Jozef Vyskoc, "Cyber Security in Slovakia," Trans. Array *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations* (Krakow, Poland: The Kosciuszko Institute, 2012), 56.
[36] Gregory Feifer, and Brain Whitmore. "Czech Power Games: How Russia Is Rebuilding Influence In The Former *Soviet Bloc," Radio Free Europe. Radio Liberty, February 26, 2013, available at: http://english.pravda.ru/russia/politics/24-01-2013/123572-russia_usa-0/.*
[37] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *Guardian*, May 16 2007; Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4:2 (2011): 49-60, available at: *http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.*
[38] Siobhan Gorman, "Georgia States Computers Hit By Cyberattack," *Wall Street Journal,* August 12, 2008, available at: *http://online.wsj.com/article/SB121850756472932159.html*; Richard Weitz, "Global Insights: Russia Refines Cyber Warfare Strategies," *World Politics Review*, August 25, 2009, available at:

http://scholarcommons.usf.edu/jss/vol7/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6

Russia's capacity for such attacks derives from having knowledgeable experts and resources.[39] Furthermore, Putin recently ordered the creation of a system that will allow the state to disable cyber attacks within Russia and "expand its presence" among the Commonwealth of the Independent States (CIS) members and its former Soviet satellites.[40]

Telefonica spokesman Hany Farghali and Milos Korenko, a cybersecurity expert in the internet-security firm Avast, blamed Russia for the recent attacks, providing Russian IP addresses and a number of botnets located in Russia as their evidence.[41] While tracking the origin of the attacks, Yandex.ru and Sezman.cz provided evidence that showed the involvement of Real Time Network (RETN), a telecommunication network located in the Russian Federation. Further investigation was not possible due to the lack of cooperation from the RETN operator.[42] Later, RETN stated that there is no data to help the investigation.[43] Moreover, Jaromil Talir, a cybersecurity expert at the Czech cybersecurity organization CZ.NIC, explains that even though it was hard to identify the perpetrator, someone with deep insight into the Czech market, who knows the most popular banks, news portals, and mobile operators, was behind the attacks.[44] It is worth noting that all data in and out of Russia is stored as metadata by the Federal Security Service (FSB) and related ancillaries, therefore RETN's claim that no data from the attacks exists is rather specious, at best.[45] The only counterarguments to this are that the FSB either deleted metadata from the date of the attacks or it truly does not have the capacity to secure Russia's networks, contrary to their claims. Irina Lagunina, a senior broadcaster at RFE/RL, an international news agency funded by the United States, and Flidr, however, remain skeptical that Russia hacked the Czech Republic.[46] They both suggest that Russia would have had more reasons to attack the Czech Republic in 2010—at the high of the contentious missile defense crisis when the relations between the two countries were tense. There has also been some speculation that the cyber attacks were designed to coincide with the inauguration of the new Czech president. Tomas Flidr debunks this by explaining that the current president's political affiliation is more or less pro-Russian, the same as the outgoing president.

Most cybersecurity professionals participating in these interviews agree that an attack origin, especially when it is a DDoS attack, is difficult to discern since hackers can easily use proxy servers to launch cyber attacks. The situation, however, has changed. Luukas Ilves, the head of the International Relations Division in the Information Security Agency at Estonia's Ministry of

---

http://www.worldpoliticsreview.com/articles/4218/global-insights-russia-refines-cyber-warfare-strategies; Evgeny Morozov, "An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar," *Slate,* August 14, 2008, available at: *http://www.slate.com/id/2197514*, as cited in Reveron, Derek (ed.) *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington DC: Georgetown University Press, 2012); Stephen Herzog, see note 44.

[39] "Cyber-attack in the Czech Republic. Thieves in the night." *Economist*, March 13, 2013.

[40] Andrei Soldatov, "FSB's Cyber Silver Bullet," *Agentura.ru*, January 27, 2013, available at: http://agentura.ru/english/projects/Project_ID/fsbcert/.

[41] Agence France-Presse, see note 2; *Economist*, *see* note 46.

[42] Narodni Centrum Kyberneticke Bezpecnosti. Denial of Service attacks in the Czech Republic in March 2013. March 2013.

[43] Jaromir Talir, Presentation on March (D)DOS attacks in the Czech Republic, May 28, 2013; Flidr, supra note 28.

[44] Jaromir Talir, Email Interview, July 14, 2013.

[45] Andrei Soldatov, "Lawful interception: the Russian approach," *Privacy International*, March 5, 2013.

[46] Flidr, see note 28; Irina Lagunina, Personal Interview, June 23, 2013.

Economics and Communications, and Kenneth Geers, a cybersecurity expert at FireEye and the first U.S. Representative to the Cooperative Cyber Defense Center of Excellence (CCD CoE) in Tallinn, Estonia, both agree that attribution is no longer a problem: it is possible to find the attack source for wealthy nations that have strong internet policing infrastructure and motivation to do so.[47] The Czech Republic however is not in the fiscal position to employ an entire army unit for the purpose of hacking (like China), solicit hacking groups in the service of the Czech Republic (like Russia), or fund major research at top universities to counter hacking (like the United States). If a hacker community were behind the March cyber attacks in the Czech Republic, they probably would have let the world know about it by boasting about their achievements and sophisticated skills via media channels. In fact, a few days after the March 11th attacks, a hacking group called Czechurity claimed responsibility for the attacks committed against the CSOB bank.[48] However, no one claimed responsibility for the March 4-7th attacks. Further, while there is a split amongst the local cybersecurity community on whether or not Russia was behind the attacks, there is a solid consensus that the attacks in the Czech Republic were a testing exercise for a larger attack yet to come. Specifically, Tomas Flidr from NBU provides two possible explanations for the March attacks. The first scenario was that someone was testing his own capabilities and then selling them—more like a show off. Another scenario is that the attacks were a cover-up, distracting people from the actual attack on another target of interest on the internet; a target that was possibly not in the Czech Republic.[49]

Situational Analysis: Czech Republic v. Russia

If Russia was indeed responsible for the first wave of cyber attacks in the Czech Republic, what are the Republic's options? The Czech Republic could avoid publically admitting that Russia or any other state can hack into its infrastructure and that it lacks the capacity to rebuff cyber attacks and thus work domestically in addressing the cyber security issue. Another option is that the Republic can express its weakness, directly or indirectly, and request cybersecurity help from its powerful allies, for instance the EU or NATO countries. There is a previous example of the dilemma the Czech Republic finds itself in: Estonia did not officially accuse Russia following a series of disruptive cyber attacks in 2007 (rather it shared its suspicion with the United States) and chose to seek assistance from NATO in developing stronger cybersecurity protection measures.[50] Such a geopolitical imbalance between Russia and Estonia might be a good lesson for the Czech Republic as the Republic has started developing stronger cyber defensive capacities in cooperation with NATO.

Moreover, similarly to Estonia and Georgia, the Czech Republic was not able to prove convincingly or unequivocally that Russia was a perpetrator, either due the lack of funding for

[47] Luukas Ilves, Personal Interview, June 20, 2013; Kenneth Geers, Personal Interview, July 11, 2013.
[48] Volynsky, see note 13.
[49] Flidr, see note 28.
[50] Wikileaks source, a U.S. cable date 6/4/07. Moreover, Prime Minister Andrus Ansip "has accused the Russian government of spearheading the cyber campaign, saying that some of the problems were traced to Russian government computers." For more information, *see* Alex Rodriguez, "Attacks on Estonia: Cyberspace sabotage blamed on Russians," *Chicago Tribute,* May 29, 2007, available at: *http://articles.chicagotribune.com/2007-05-29/news/0705290081_1_estonian-officials-estonian-defense-ministry-russian-officials*; Jim Michaels, "NATO to Study Defense against Cyberattacks," *USA Today*, June 15, 2007, available at: *http://www.usatodayeducate.com/wordpress/?dl_id=9*.

http://scholarcommons.usf.edu/jss/vol7/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6

origin attribution in its cyberspace, politico-economic considerations (gas and oil for Estonia and Czech Republic, avoidance of separatist conflicts in Georgia) or a simple lack of courage to accuse Russia outright. Making accusations with a lack of concrete evidence can cause these smaller nations to provoke Russia, or any other nation with far more financial and military resources, to willfully and brazenly violate the smaller states' sovereignty as a show-of-force, as evidenced by Russia's behavior in Estonian and Georgia. The worst-case scenario for the victim-country would be to wrongfully accuse Russia, or another world power, of sovereignty violations, potentially provoking a severe diplomatic crisis.[51]

Similar to Estonia, the Czech Republic has a Mutual Legal Assistance Treaty with Russia and can accuse Russia of non-cooperation if the latter refuses to help in the investigation process—a likely scenario.[52] The Republic, however, never asked for Russia's assistance, as the damage from the March 2013 attacks was minimal.[53] Furthermore, after witnessing Russia's refusal to help Estonia investigate the 2007 Estonian cyber attacks, despite the Mutual Legal Assistance Treaty between those two nations, the Czech Republic might have decided to cooperate with NATO rather than asking Russia for help.[54] As such, only a few private companies in the Czech Republic took the initiative to investigate the attacks and are currently working with their Moscow offices.[55] Similar to Estonia, the Czech Republic is possibly choosing to not blame to Russia because of the risk of undesirable Russian escalation (such as natural gas sanctions or military posturing); thus, the best option for the Republic is to follow the Estonian example and cooperate with NATO, which has more resources to help the Czech Republic develop cyber capabilities, implement cyber protective measures, and prevent future attacks in the online environment.

Russian Cybersecurity Capacity: Real or Imagined?

If the Czech attacks did in fact originate in Russia and the Russian state is not responsible, then it could be viewed as a failure of the Russian state's ability to police its cyberspace. Recent Russian cyber history shows that Moscow was at the very least aware of the illicit activities and may have lent its unofficial support by not exercising its wide-ranging and highly capable Internet policing arm in dealing with the attackers. The post-Soviet Russian state began using its domestic hacker community in the 1990s to do the government's bidding, since it was easier to disguise the misbehavior of non-state actors than state-sponsored activities.[56] Such cooperation continues to benefit both parties as the hackers enjoy a certain degree of immunity and fill their pockets with Western money, while the Russians can anonymously utilize the hacker's talent at little to no significant fiscal cost. Lagunina agrees with Arkady Pildes that the Russian government is using hackers for its own objectives. To show a long-term relationship between the state and the hacker-community, she cites the attacks on the Prague branch of the RFE/RL

[51] Rezek, see note 11.
[52] "Russia Country Profile - Legal Frameworks," *International Centre for Asset Recovery*, available at: *http://www.assetrecovery.org/kc/node/50560f43-c065-11dd-b3f1-fd61180437d9.0;jsessionid=E578782425DD8D841FADF9FDD3F1395E.*
[53] Krulik, see note 11.
[54] Lagunina, see note 54; Russia Country Profile - Legal Frameworks," see note 62.
[55] Such as Deloitte, Cerveny, see note 31.
[56] Sergei Modestov, "Na Nevudimom Frontye-Aktivizatsiya boyevykh deystviy" ("At the Invisible Front –Warfare Activization"), *Delovoy Mir (Business World)*, February 24, 1994, 7.

that occurred a decade prior. The investigation into this attack, during which the organization's FTP server was crippled, discovered that the IP addresses were located close to the Kremlin.[57] When RFE/RL wanted to find out more about these addresses and asked Russia for help, everything was blocked, preventing further investigation. Lagunina and Pildes both agree that a similar technique was used during the Estonian and Georgian cyber attacks.[58] Edward Lucas, International Editor of *The Economist,* defines a hybrid model as representative of the state (FSB, GRU)-hackers' relations in Russia.[59] Specifically, hackers will work for the FSB part-time, conducting semi-criminal activities such as identity theft, spear-fishing, hacking, or looking for open ports. These hackers are not afraid of prosecution, since the state is their *krysha ("roof").* At the same time, others that work for the government are involved in the private sector and can use the private sector's superior resources on command.[60] Such a system, in which different employees have different motives and allegiances make it difficult for prosecutors to place blame for any given misdeed, especially when it comes to the online environment with its complex exigencies.

Pildes succinctly describes the state-hacker relationship by using an old Russian saying that characterizes the Soviet times: "*Vlasti znaiut kto, gde i chto" ("The state knows who, where, and what").*[61] He added that the state always watches the hackers' activities but waits for a specific moment and "when that moment comes, no matter what [the hackers] are doing, the state will find a motive to touch [them]."[62] Not surprisingly, the Russian government is not in a hurry to adopt countermeasures, as employing hackers is convenient. As such, this creates an inverse incentive for illicit hacking to continue.[63] The FSB even began indirectly offering jobs to hackers who have been caught and are awaiting sentencing, an activity that is not uncommon even in the West.[64] Giles specifies that recruitment is mostly done via *posrednik* ("middleman") organizations that have connections to the FSB, and he pointed out the "School of Patriotic Bloggers" as such an example.[65] Led by Nikolai Starikov, this school is a propagandistic organization that provides lectures and detailed descriptions to amateur and professional hackers on how to counteract the activities of *protivnikov Rossii* ("*those who are against Russia").*[66] The School is not only active online. Its main lecturers are constantly travelling all over Russia looking for young patriots who are willing to police websites from Western influence. He continues that it would be specious to say that the FSB or the Russian state is directly recruiting hackers, as it is not as evident as it is in China.[67]

---

[57] Lagunina, see note 54; Arkady Pildes, Personal Interview, June 24, 2013.
[58] Ibid.
[59] Edward Lucas, Skype Interview, July 8, 2013.
[60] Ibid.
[61] Pildes, see note 70.
[62] Ibid.
[63] Lagunina, see note 54; Pildes, see note 70.
[64] Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, October 16, 2008, available at:
http://voices.washingtonpost.com/securityfix/2008/10/report_russian?hacker_forums_f.html?nav=rss_blog6.
[65] Keir Giles, Skype Interview, July 27, 2013. For more information about the School of Patriotic Bloggers (Школа блоггеров-патриотов), *see http://nstarikov.ru/blog/9793.*
[66] Nikolai Starikov, "Школа блоггеров-патриотов. Лекция 1," available at: *http://nstarikov.ru/blog/9793.*
[67] Ibid.

http://scholarcommons.usf.edu/jss/vol7/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6

Russia's indifference towards its domestic hackers provides them with impunity and creates additional challenges for developing countries. If developed countries that have resources and capabilities were to aggressively prosecute their domestic hackers, then developing counties would likely suffer fewer attacks. On the other hand, when a developed country closes its eyes on its hackers, developing nations must either suffer from cyber attacks or cooperate with their allies, since there is a lack of international legislation regulating cyber crime.

Options for the Czech Republic

Most small nations, similar to the Czech Republic, lack the fiscal resources to go toe-to-toe with an APT launched from the United States, Russia or China. Small nations should look to cooperate with each other in order to bolster themselves collectively in the face of greater threats, whether those threats are state sponsored or individually acted, and then work with larger nations as a united block. Though the Czech Republic is already affiliated with groups (notably NATO and the EU), the lack of a collective cyber defense paradigm and the continuing zeal for national Internet sovereignty makes these collective organizations useless in mitigating APTs from public or private actors. This could change with some sacrifices by affiliated nations and a renewed drive for collective defense against twenty-first century threats. Therefore, these are the recommendations that are specifically tailored for the Czech Republic but could be readily adapted by other nations.

Cooperation with the EU and NATO

Cooperation with the EU and NATO is the best and the most important step for the Republic since it lacks the proper resources to defend itself. A recently created European Cybercrime Center should develop a better platform for coordinating cooperation between the twenty-seven EU member states and help them develop new technologies to combat cyber crime, as well as "engage [their] businesses to share information and be more aware of potential threats."[68] Moreover, European nations can use Smart Defense introduced by NATO to coordinate all actions on the basis of the "pool and share" rule, which facilitated the sharing of the best solutions amongst all the allies.[69] Lastly, Czech cyber security experts should become more involved with work of the EU's European Network and Information Security Agency (ENISA), which has been expanding in light of cyber attacks, which have increased in both frequency and magnitude, and has significant pooled resources to mitigate the effects of cyber attacks. Additionally, the Czech Republic could also strengthen ties with the NATO Cooperative Cyber Defense Center of Excellence and eventually become a member of that organization. Such cooperation could enhance technical competency, and make the Czech Republic more resilient to future attacks. The first step in this process for the Republic should be the ratification of The Council of Europe Convention on Cybercrime.

Need for better cyber protective measures

[68] Ben DiPietro, "European Cybercrime Center to Focus on Cooperation, Upgrading Technology," *Wall Street Journal,* Januanry 14, 2013, available at: *http://blogs.wsj.com/corruption-currents/2013/01/14/european-cybercrime-center-to-focus-on-cooperation-upgrading-technology/*.
[69] Świątkowska, see note 27. For more information on *Smart Defence*, see *http://www.nato.int/cps/en/SID-8A152E11-04F93301/natolive/topics_84268.htm*.

The first steps that the Czech Republic has taken in implementing cyber protective measures are significant but they are not enough considering the fact that cyber attacks become more sophisticated every minute. Even though interviewees have lots of recommendations of specific products (each promoting their companies' products), the efficacy of specific products should be evaluated before implementation. Martin Koldovsky identifies two issues that prevent the implementation of protective measures: a lack of financial resources to purchase the equipment and the public's perception of this technique.[70] While the first reason is self-evident, the second might need a bit of explanation. Most Czechs rely on a computer specialist to guide their software and hardware needs as it relates to efficiency and protection. The installation of automatic response equipment such as smart servers and advanced firewalls in lieu of the firm expert may not be well received. Moreover, most companies have not had a major problem yet, thus they do not want to spend their limited budgets for such expensive technologies.[71] Considering the situation in the country, changing this unfavorable outlook towards new protective techniques should be the first measure that will potentially serve as a stepping-stone towards implementing new cyber security measures. This could be achieved through workshops and awareness seminars during which potential damage to companies without adequate protective measures can be demonstrated. Following this, companies should try to seek additional funding from the government or any outside sources, including regional and international agencies. The Czech Republic needs to go from reactive (human IT) to proactive (hardware and software in concert with human IT) in order to mitigate the effects of the next wave of attacks.

Need for qualified specialists in a public sector

New hardware and software defenses will not enough in and of themselves to protect the Czech Republic against the next cyber attack. These new technologies will require new types of experts that are not currently present in the Republic and there will be a steadily increasing need for them as the republic reaches it Internet saturation targets. As these experts will need advanced training and re-training and because the Czech Republic is one of many nations expecting double-digit internet reach expansion in this decade, cooperation with other countries to train this new generation of experts could both keep the cost of training low while increasing member of experts rapidly. Evan Lesser, managing director at ClearanceJobs.com, points out that the most capable responders to the cyber threat are "not government employees, they [are] in private industry."[72] The Czech Republic, however, lacks these qualified specialists even in the private sector.[73] Working for private companies, these employees only deal with cyber threats affecting their companies' work. Thus, if the government is affected, these specialists are generally not qualified to deal with the issue. Moreover, this scarcity in skilled experts might jeopardize international cooperation.[74] Therefore, there is an urgent need for the Czech Republic government to provide incentives for cyber experts to work for them, as national security should be a higher priority than individual order of a private client. The most obvious but most

[70] Martin Koldovsky, Personal Interview, March 19, 2013.
[71] Ibid.
[72] "It's hard to know where to turn during a cyber attack," *Nextgov*, available at: *http://www.nextgov.com/cio-briefing/wired-workplace/2013/03/its-hard-know-best-place-turn-during-cyber-attack/62074/.*
[73] Rezek, see note 11; Filip Volavka, Personal Interview, March19, 2013; Cerveny, see note 31.
[74] Świątkowska, see note 27, 8.

http://scholarcommons.usf.edu/jss/vol7/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6

challenging step would be the reevaluation of the salary table and implementation of new incentives that consider experience and expertise of a state employee.

Public-Private Partnership

As information travels through the space owned by private companies, states should continue to enhance their ties with private companies and establish working agreements under which these companies are obliged to provide key information to investigators. The "Cyber Silk Road" model, for instance, offers infrastructure providers incentives to cooperate with cyber attack investigators. In the case they refuse to do so, they can suffer legal consequences.[75] Moreover, a recently developed initiative in collaboration with various universities, including the University of Brno, will offer selected students an internship for college credit accompanied by a small stipend in hopes of attracting talented individuals to work for the government.[76] Such academia-government partnerships are nascent steps in developing cooperation between various cyber actors. Lastly, the Czech Republic's private sector is not as robust as its near neighbors, such as France or Germany; therefore it would be prudent for the country to engage strong global internet firms that could help develop better network security and more resilient network infrastructure. Government-sponsored investment opportunities in the country, such as tax credit, could be used to entice major global tech firms to invest in the Czech Republic market.

Grey-area Options

It would be worthwhile to compare the alternatives, namely three primary models for dealing with cybersecurity: the use of illicit privateer hackers, uniformed military hackers, or government contractors. The Russian model of dealing with hacking is to covertly fund private citizens and utilize their hacking talents in the service of the Kremlin. As this research has shown, this model has been successful, though there is the significant potential that these individuals might start using their skills against the state. For instance, in the Soviet-Afghanistan War, a young Usama bin Laden was used as a mercenary by the Pakistani ISI spy agency (with American weapons and funding), but eventually betrayed his contractors in Islamabad and Washington by becoming the zeitgeist of a modern jihad. Such is also true of the Russian *suki* convict-veterans who eventually formed the core of the Russian mafia.[77]

China combats hackers by first training in-house military elites. Specifically, China's alleged 2nd Bureau of the People's Liberation Army (PLA), 3rd General Staff Department's (GSD) utilizes an unknown number of people in a twelve-story building to hack private and public networks worldwide in the name of Chinese defense.[78] This model works for China since it has the human capital and financial resources to sustain such an army. Furthermore, its economic position in the world offers China both plausible deniability and leeway to continue these attacks as many

[75] Goodman, see note 17.
[76] Krulik, see note 11.
[77] "People in the News. Osama bin Laden," *CNN World*, available at: *http://www.cnn.com/CNN/Programs/people/shows/binladen/timeline.html.*
[78] Dan Mcwhorter, "Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators," *Mandiant M-unition*, February 18, 2013, available at: *https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/*; Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence,"*Journal of Strategic Security* 4:2 (2011): 1-24, available at: *http://scholarcommons.usf.edu/jss/vol4/iss2/2/.*

nations, including the United States, choose not to publicly accuse China in order to protect mutually beneficial economic relationships. Men and women in the Chinese model are sworn in as agents of the state in the service of their homeland's defense, which can be a deterrent from treason, giving strength to this approach. Though China has had remarkable success with its illicit military operations, this model is not feasible for other states, both large and small. U.S. Army Private Bradley Manning, for example, took an oath to serve the United States and yet his consciousness encouraged him to steal and reveal classified information as a protest against his nations' questionable activities in Afghanistan.[79] Data, unlike a cruise missile or a nuclear warhead, is highly portable and agents with questionable loyalties and/or motivations can acquire many terabytes of sensitive information and distribute it to anyone for any reason. Clearly, the military model of cybersecurity has as many risks as benefits. The Chinese model also is impractical for smaller nations such as Estonia, Georgia and the Czech Republic whose combined armed forces are smaller than the amount of regulars in the Chinese PLA alone. Even if the Czech Republic was to invest all its available resources into the development of a Chinese-style offensive cyber army, such a redirection of resources will detract from other necessary efforts, therefore bolstering defense in one area while leaving critical vulnerabilities in others. Larger countries such as Russia can then exploit those vulnerabilities, turning any smaller nations' cyber defense strategy into a veritable Maginot line.

The long-standing U.S. contractor model is worthy of debate as there are issues of mission adherence and cost effectiveness that are in need of investigation. Industrial failures do not happen that often, but when failures do occur, they are catastrophic—something that Edward Snowden has demonstrated. Outside of the potential for future leakers, there are also questions of scope and scale when dealing with classified materials across dozens of private firms of varying sizes. For nations creating such structures from scratch, the potential risks may not outweigh the potential for cost savings over government employment. Additionally, the cost of reputable contractors may be out of reach for many nations. Mandiant, the company that has been at the forefront of investigating Chinese hacking, may be out of the price range for countries with limited pecuniary resources since Mandiant's analysts start at $650 dollars an hour.[80] Additionally, Mandiant specializes in reactive recovery operations following an attack and often advises victims to replace compromised computer systems. For wealthy governments and cash-flush private companies, this may not be an issue; small nations and private firms, however, most likely would balk at having to throw out entire server banks.

Lessons for the Global Internet Community

The research findings are significant for the field of international relations as it shows how traditional and non-traditional actors use technology as a non-traditional means to violate state sovereignty. The lessons learned from the Czech Republic's recent cyber attack are useful for other developing nations because the World Wide Web erases any physical borders among them, making them vulnerable to future attacks. In lieu of recent cyber attacks across the globe,

[79] Tim Weiner, "Manning's Crime: Stealing the Dirty Secrets of War," *Bloomberg News,* July 30 2013, available at: *http://www.bloomberg.com/news/2013-07-30/manning-s-crime-stealing-the-dirty-secrets-of-war.html*.
[80] Brad Stone and Michael Riley, "Mandiant, the Go-To Security Firm for Cyber-Espionage Attacks," *Bloomberg Businessweek*, February 7, 2013, available at: *http://www.businessweek.com/articles/2013-02-07/mandiant-the-go-to-security-firm-for-cyber-espionage-attacks.*

http://scholarcommons.usf.edu/jss/vol7/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.6

internet-sophisticated nations proved to be as vulnerable to attack as nations that in inchoate phase of their Internet development. This case study demonstrates the importance of cooperation between these powerful nations, as states will continue to be attacked until they create regulations for the online environment that reflect common approaches to Internet security. No matter how technologically advanced a nation is, its cyberspace remains vulnerable until international agreements that regulate behavior in the online environment are achieved.

Conclusion

The Internet is a powerful tool that has created numerous opportunities and vulnerabilities over the past two decades. Nations with abundant resources and capabilities can use this tool to gain an advantage over each other and maintain their advantage over smaller nations. Such an advantage was demonstrated using the case study of the Czech Republic, a developing country that faces domestic complexities while addressing cybersecurity, a still-emerging field with many questions but very few answers. Many small countries, similar to the Czech Republic, face similar challenges as they do not have the ability to accuse their perpetrators and do not have the resources to prosecute cyber offenders in order to deter future cyber attacks. This case demonstrates that the best option for developing nations is to cooperate with powerful nations that can help them defend themselves. Moreover, it is in every nation's best interest to put aside their insecurities and disagreements and start cooperating for the creation of a safer, more secure, cyberspace that can confidently be shared by all legitimate participants.