The Estonian Cyberattacks

Andreas Schmidt

Delft University of Technology

Chapter prepared for the edited book *The fierce domain – conflicts in cyberspace 1986-2012*, edited by Jason Healey, Washington, D.C.: Atlantic Council, 2013 (forthcoming).

For three weeks from April 27 until May 18, 2007,[1] components of the Estonian Internet infrastructure were subjugated to Distributed Denial of Service (DDoS) attacks, website defacements, DNS server attacks, mass e-mail, and comment spam. These attacks seem to be the first that were possibly directed as a coercive instrument in a political conflict against a nation. At the time of the attacks, Estonia was entrenched in a domestic conflict between the newly elected government and its supporters on the one hand and the Russian ethnic minority group on the other. In addition, the long-standing conflict with Estonia's former occupant power, Russia, had culminated in heated diplomatic exchanges at a time when Russian-US relations approached their post-Cold War bottom.

The incident is noteworthy for more than its geopolitical implications. It also sheds light on organizational aspects of cybersecurity and the role of global technical communities to reestablish the Internet‘s functionality after an attack.

The chapter offers a descriptive account of the attacks, the damages that they inflicted, and the responses made. This narrative is supplemented by an analysis of the political circumstances of the attacks, the discussions that the attacks spurred, and some recapitulating remarks.

Monument debates

In January 2007, the Estonian government announced that it would move a World War II monument from the center of Tallinn to a military cemetery in the outskirts of the city. Erected in

[1] At the end, the attacks frayed out a bit, hence the end is not as sharply delineated as the beginning. Therefore, in some descriptions May 23 is given as the end date and 3 ½ or 4 weeks as the overall duration.

1947, when major affairs in the Estonian Socialist Soviet Republic were controlled from Stalin's Kremlin, the "Monument To the Fallen in the Second World War" depicts an unnamed soldier wearing a uniform of the Red Army, with a helmet in is left hand, and his head slightly bowed as if he was mourning his nearly 11 million fallen comrades.[2] After Estonia regained its full political sovereignty in 1991, the monument became a point of conflict in domestic Estonian affairs. Many Estonians regarded the Bronze Soldier, which was located at a busy intersection close to Tallinn's picturesque historic center, as a symbol not of the achievements of the Red Army in WWII, but of its subsequent role as a suppressor of Estonian independence. Russian-Estonians begged to differ. Unsurprisingly, the monument emerged as the site where different interpretations of the role of the Red Army were expressed in demonstrations. The date of May 9, the Russian V-Day,[3] became notorious for verbal clashes between Soviet war veterans and Estonian-Russians on the one side and conservative Estonians on the other. After years of repeated rallies, discussions about the future of the monument and demands for its removal grew more prominent in 2006.[4]

It didn't go unnoticed in Moscow that its former Soviet republic was about to cut ties to the Russian interpretation of Estonia's WWII and post-war history. In January, the Russian Upper-House filed a resolution demanding that their Estonian parliamentary peers halt legislation that would remove the monument. On April 3, Russian First Vice Prime Minister Sergei Ivanov made a plea to boycott Estonian goods and services, though this bullying attitude was not shared by those in Russia's foreign policy circles.[5] The conflict was about Estonian identity, relations between Russia and Estonia, and the perception of World War II.[6] For Russians, it was the Red Army that wrestled down the German war machine in the bloody battles of the "Great Patriotic War," which cost the lives of approximately 27 million Soviet citizens.[7] In the eyes of (some)

[2] Hosking, *Rulers and Victims, 206*.

[3] The Allied Forces had summoned Wehrmacht General Jodl to Reims, France on May 7, 1945 to sign the capitulation, to be effective on May 8, 23:01 CET, i.e., after midnight in Moscow. In addition, the Soviets held another signing ceremony in Berlin on May 9, close after midnight CET. Kershaw, *Hitler*, 1073-75.

[4] Alas, "May 9 Protestors Call for Removing Bronze Soldier Statue."

[5] "Here We Go Again."

[6] Myers, "Debate Renewed: Did Moscow Free Estonia or Occupy It?"

[7] Kosachev, "An Insult to Our War Dead."

Estonians, however, the Nazi occupation was only relieved by a five-decade long occupation by the Soviets that continued the suppression of the Estonians, who were striving for autonomy.[8]

After smoldering for a time as a divisive and emotional issue in Estonian politics and public discourses, the monument eventually became one of the core subjects in the lead-up to the Estonian parliamentary elections that were held on March 4, 2007. "War graves are no place for day-to-day politics," warned President Toomas Hendrik Ilves, a Social Democrat, but to no avail.[9] The Union of Res Publica and Pro Patria, a conservative opposition party, lobbied for a bill prescribing the removal of the monument. Trailing in the polls, the incumbent Prime Minister Andrus Ansip and his Reform Party supported the controversial bill in February, fearing an electoral setback for the forthcoming elections.[10] The elections confirmed the Prime Minister's new term, and the Reform Party finished ahead[11] of the social-liberal Center Party and its candidate, who preferred a less controversial approach regarding the monument. In March, Ansip's new government immediately laid the legal ground for the removal of the Bronze Soldier.

On April 26, Estonian authorities fenced off the statue in the center of Tallinn. A day later, they removed the statue, exhumed the bodies of the Red Army soldiers buried underneath it, and transferred them to a military cemetery in the outskirts of Tallinn.[12] Unsurprisingly, the removal angered Russians, Estonia's ethnic minority, and citizens of the Russian Federation alike. On the Russian side, the chorus of outrage was spearheaded by President Putin, who fiercely criticized the Estonian decision. In Tallinn, streets were filled with protesters, rallying against the decision of the Estonian government. Estonian police forces arrested hundreds of protesters.[13] In the late

[8] Socor, "Moscow Stung by Estonian Ban on Totalitarianism's Symbols."

[9] Alas, "Soldier Fails to Sway Elections."

[10] *Ibid*.

[11] Alas, "Reformists Pull Off Surprise Victory, Consider Dumping Centrists."

[12] "NATO Sees Recent Cyber Attacks on Estonia As Security Issue."

[13] Adomaitis, "Estonia Calm After Red Army Site Riots, Russia Angry."

evening of the day of the monument's removal, on Friday, April 27,[14] first signs of cyberattacks appeared on the monitoring screens of Estonian IT operators.

Early Attacks

Starting at around 10 pm, Estonian organizations faced several kinds of attack on their servers which were used for e-mail, the Web, domain name resolution, and other Internet services. Systems slackened or stalled under unusually high data traffic. Internet sites suffered from Web defacements. Email inboxes were filled with even more spam and phishing emails.[15]

Political institutions were early targets of the attacks. Estonian Prime Minister Andrus Ansip and other leading politicians were spammed.[16] The email services of the Estonian parliament had to be temporarily shut down, as they were no longer able to handle the unusual data payload.[17] The Estonian news outlet *Postimees Online* fell victim to two DDoS attacks on its servers and had to close foreign access to its networks, thereby limiting the chances for Estonians to make their voices heard abroad.[18] In addition, discussion forums on Postimees Online were spammed by bots with comments badmouthing and insulting the Prime Minister. The president of Postimees Online likened the cyberattacks to an "attack on neutral and independent journalism." [19]

While defacements of governmental websites created embarrassment for the sites' owners and symbolically undermined political institutions, they hardly constitute a major blow to the society and its security. The main causes for concern were the DDoS attacks on the Estonian

[14] In their joint presentation, Gadi Evron, a known ICT security expert who arrived in Tallinn after the attacks had peaked, and Hillar Aarelaid, head of the Estonian CERT, spoke of "Saturday, the 26th of April, 22:00" as the day when the attacks started. But immediately after this, they mentioned "Saturday, the 27th of April, 02:00" as the beginning time. Evron and Aarelaid, "Estonia: Information Warfare and Lessons Learned." However, in 2007, the last Saturday in April was the 28th. In a post-mortem journal article, Evron stated that the attacks started at "10:00 p.m. on 26 April 2007." Evron, "Battling Botnets and Online Mobs," 121-126. Street demonstrations that later led to riots took place on April 26 and April 27. Presentation slides made by Merike Kaeo, a US-based Estonian security expert, contain a graphic of web traffic between Friday, 0:15 am, and Saturday noon, according to which traffic first abnormally increased on Friday night around 10:15 pm, but culminated no earlier than on late Sunday, April 28. Interviewees confirmed that attacks started on a Friday, i.e., on April 27.

[15] For prior descriptions of the Estonian incident, see also Herzog, "Revisiting the Estonian Cyber Attacks," 4; Landler and Markoff, "In Estonia, What May Be the First War in Cyberspace"; and Tikk, et al., *International Cyber Incidents - Legal Considerations*.

[16] Berendson, "Küberrünnakute Taga Seisavad Profid."

[17] Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic."

[18] "Hansapanka Tabas Küberrünne."

[19] Berendson, "Küberrünnakute".

infrastructure, as they endangered the availability and functionality of services crucial to the functioning of Estonian society.

Internet traffic exceeded average-day peak loads by a factor of 10, resulting in malfunctions or non-availability of Internet services.[20] The Estonian government was the most notable among the institutions affected. Its website, valitsus.ee, was not available for eight consecutive hours in the afternoon of April 28. For the following two days, response times often took an unusually long time, eight seconds and more, if the site was available at all. Statistics from Netcraft.com, a website that gathers information about the up- and down-times of webpages, revealed that the website failed to respond in 84 of 166 cases until Monday early morning.[21] Among the other affected websites were those of the Prime Minister (peaminister.ee), the Ministry of Economic Affairs and Communication (mkm.ee), the Ministry of Internal Affairs (sisemin.gov.ee), the Ministry of Foreign Affairs (vm.ee), and the Estonian Parliament (riigikogu.ee).[22]

Boot-up of the Estonian Response

The attacks didn't come as a surprise to the Estonian security community. They had seen it coming. "When there are riots in the streets, they will eventually go cyber," was an assessment

[20] Aarelaid, "Overview of Recent Incidents."

[21] Hyppönen, "Update on the Estonian DDoS Attacks."

[22] Hyppönen, "Unrest in Estonia." Further domains that were attacked included: the Estonian Patent Office (epa.ee), the Estonian Defense Forces (mil.ee), the Estonian Academy of Music and Theatre (ema.edu.ee), Tallinn University (ehi.ee, tpu.ee), the Estonian Business School (ebs.ee), Tallinn University of Technology (est.ttu.ee), a Yellow pages website (infoatlas.ee), and a URL shortening service (zzz.ee). Aarelaid, in "Overview" (confirmed in an interview with the author), that Berendson mentioned the following additional targets: "the University of Tartu, the Estonian Radio, the Estonian Shipping Company, the Woodman Pärnu furniture company, and a real estate company called Rime." Berendson, "Küberrünnakute." However, we have no statistically sound information about the effects on the availability of those websites. Websites marked as available in Hyppönen's brief analysis were: the Party of the Prime Minister (reform.ee), the Ministry of Agriculture (agri.ee), the Ministry of Culture (kul.ee), the Ministry of Defense (mod.gov.ee), the Ministry of Finance (fin.ee), the Ministry of Justice (just.ee), the Ministry of Social Affairs (sm.ee), the Ministry of the Environment (envir.ee), and the Estonian Police (pol.ee). Hyppönen's analysis is ambiguous as to whether the websites marked as reachable had been attacked not at all, before or after the period of time analyzed, i.e., for Saturday, April 28, 2007. In general, there is no consistent, conclusive assessment of the exact downtimes of organizations belonging to the Estonian infrastructure during the entire three weeks of the attacks. It is noteworthy that an attack on the web-services of an organization does not necessarily affect its functionality. E.g., the attacks had "no impact on the Estonian military forces or national security apparatus," as a report by the US-based National Defense University holds. Miller and Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," 3.

shared by many in the Estonian security community.[23] But it wasn't only intuition that led to the expectation of some sort of cyberattacks were coming. The message was spreading within both Estonian and wider international Internet security communities in mid-April that commenters were calling within Russian-language forums for low-intensity cyber call-to-arms, in an apparent attempt to find comrades who would help to initiate DDoS attacks against organizational pillars of the Estonian society.[24]

Estonia had a well-connected and prepared national ICT security community in place by the time the attacks commenced. As early as the late 1990s, banks had started collaborating and exchanging information on cyber attacks. At first, ICT security departments cooperated, ignoring legal regulations (exchanging information among banks was forbidden by Estonian law). Eventually, executive decrees and later legislation paved the way to legality for the actions of the banks' ICT security staffs. By the early 2000s, the efforts of the banks' information security staffs were supplemented by actions taken by their peers in ISPs, telcos, energy companies and certain major companies from other sectors. "We," an Estonian expert recollected concerning the community's sentiment, "started realizing that we had created a small working group. We were

[23] Estonian ICT security expert interviewed by the author. Empirical findings in this chapter are, next to the literature cited, based on semi-structured one-on-one interviews conducted by the author with persons directly involved in the response activities. Selection criteria for the Interviewees were their roles in the response activities, obviously their willingness to conduct such interviews (not everyone responded, unsurprisingly), their ability to provide additional explanations on technological, organisational, or political circumstances. Most interviewees worked as security professionals in organisations that were somehow affected by the attacks or were otherwise involved in the response activities. As some interviewees have asked for anonymity, the general policy in this chapter is to not name interviewees, unless they have already become public figures anyway by previous press coverage. The interviews for the Estonian case were conducted in 2011 and 2012 during research trips to Estonia, California and at various other places in Europe, usually on the occasion of Internet (security) conferences such as the Internet Governance Forum, TF-CSIRT, GovCERT NL and FIRST meetings, and closed gatherings of the Internet security community. In 2013, I had a few additional background conversations or follow-up interviews.

[24] Global network security communities learned about the call-to-arms in the Russian-language forums before the attacks actually commenced, just like their Estonian peers. Atlantic Council of the United States, "Building a Secure Cyber Future." It took these communities some three weeks to establish direct communication channels. Among the reasons for this were unawareness of one another's existence, mutual lack of trust, and issues that appeared to be more important than contacting peer communities. Based on existing links to their Estonian peers, some European technical experts shared their insights on the ongoing scheming within the Russian online forums with Estonian security staff by mid-April; i.e., weeks before the latter were granted access to communication channels of global mailing-list-based communities. Apparrantly, some Russian web forums are constantly monitored by various Western parties, who are interested in Russia-based cyber-crime, malware, underground economies, espionage, and other suspicious activities.

starting to protect the Estonian national critical infrastructure."[25] Not much later, Estonia's informal ICT security community linked up with traditional security instititions. With the advent of Internet-based elections in the early-mid 2000s, a task force consisting of security experts from ISPs, election authorities, police, intelligence services, and others was formed to prepare for potential attacks on the elections. Exposing the vulnerabilities of electronic voting systems had become a favorite pastime among hackers worldwide, an activity which severely hurt emerging voting systems businesses. A member of the task force responsible for the security of Internet voting in Estonia admitted that their voting system was as secure or insecure as the PCs of the voters.[26] The task force tried to reduce these risks by continuous monitoring of the Estonian Internet during the elections.

The same task force was re-established for the 2007 elections. A good month after the national election was held without major technical security issues, the informal Estonian community was on alert, again. They expected May 8 to be the most likely date for a spill-over of the offsite riots to the digital sphere: "We had everything ready."[27] Persons close to the Ministers of Defense and the Interior were informed about possible DDoS attacks, and Estonian intelligence was also informed, as their operatives were part of the informal Estonian Internet security information exchange system.

Despite the inability to centrally monitor national Internet services, it soon became obvious to technical operators in Estonia that the websites of a number of local institutions had fallen victim to DDoS attacks. On Russian-language web forums, descriptions of how to harm Estonian servers and Windows command shell scripts were published, along with pleas to run those scripts at a certain point of time.[28] Thousands of people running these scripts simultaneously may result in web-traffic that over-stretches the capacity of those servers. This brief, initial attack phase, which relied on humans executing the scripts, only lasted for a few days.

Four hours after the attacks had commenced, at 2 am in the early morning of Friday, April 27, operational teams responsible for governmental servers had realized from mutual updates by

[25] An Estonian interviewee.

[26] Sietmann, "22C3: Pro und Kontra e-Voting."

[27] An Estonian interviewee.

[28] Compare Aarelaid, "Overview." For an example posted in a Russian website, see: http://theologian.msk.ru/thread/list00350.php (last accessed in August 2012).

telephone that some government websites were being exposed to Internet traffic exceeding normal traffic by 100 to 1000 times. Servers could not cope with the enormous traffic. Hence, the operational teams decided to move websites to “well-defended” web servers, scaled to handle the excessive traffic.[29] What had started as an operational IT security issue (DDoS attacks are almost daily business) turned into a national security situation three hours later, when the chief public relations person of the Estonian Defense Ministry stated around 1 am on April 28, “We are under cyberattack.”[30] His superior, the Estonian Minster of Defense Jaak Aaviksso said, “It turned out to be a national security situation.”[31]

This "security situation" was subsequently mitigated by the Estonian community of technical experts, who—at the beginning—acted with mild support from their international peers. When the attacks commenced, CERT-EE naturally became the central hub for information exchange and coordinated some of the defensive measures of operational IT units in Estonian organizations. According to Lauri Almann, Estonia’s then Permanent Undersecretary of Defense, “we put together a team of experts from our Departments of Commerce and Communications, the military, and the intelligence community, led by Estonian CERT.”[32] Hillar Aarelaid, one of the then two full-time staff-members and head of CERT-EE,[33] listed all of the actors involved in the response: the “national crisis committee, DNS / TLD, ISPs, telcos, banks, cyberpolice, intelligence, counterintelligence, CERT-EE, [the] community, some friends, [the] Government Communication Office, [the] National Security Coordinator, [the] Ministry of Foreign Affairs, MoD, ‘helpers’, NATO, DHS, [and the] embassy’s [sic]."[34] The most significant role in the technical response activities certainly was handled by the Estonian CERT.[35]

[29] Evron and Aarelaid, "Estonia."

[30] Kash, "Lessons From the Cyberattack on Estonia. Interview with Lauri Almann, Estonia's Permanent Undersecretary of Defence."

[31] Cited by: Landler and Markoff, "In Estonia."

[32] Kash, "Lessons From Cyberattack."

[33] Randel, "CyberWar in Estonia 2007 - History, Analysis."

[34] Aarelaid, "Overview."

[35] Gadi Evron’s take on who the decisive actors were in responding to the attacks was: “The heroes of the story are the Estonian ISP and banking security professionals, and the CERT (Hillar Aarelaid and Aivar Jaakson).” Evron, “[NANOG] An account of the Estonian Internet War.” Various interviewees criticised the centrality of CERT-EE, as that had established a single-point of failure in the Estonian response organisation. This organisational vulnerability could have been exploited by the attackers.

Collaboration with domestic actors was facilitated by previous collaboration and Estonia's unique situation. In a country with 1.4 million inhabitants (about 400,000 of them gathered in the capital, Tallinn), geographic proximity and naturally close social ties facilitate defensive *ad-hoc* collaboration. The Nordic sauna culture, which according to Nokia's then new CEO Stephen Elop had led to the demise of Nokia,[36] came to the rescue for Estonia. Meeting peers in hour-long gatherings of alternating sauna and beer-drinking sessions (which were dubbed the "beer & sauna protocol") helped to formulate a degree of trust among the Estonian experts that allowed them to collaborate seamlessly during the attacks.[37] On April 30, Estonian experts came together for a joint meeting, representing organizations such as ISPs, mobile Telcos, operators of the Estonian TLD and DNS, banks, police, and envoys from the government's Security and Information Boards. This group met only twice in person during the incident, as most of the collaboration was done online via IRC, wikis, email messages, and after-work beer-and-sauna sessions.

The Second Phase

In the second and main attack phase, the coordination of the attacks no longer depended on forum communication and synchronized human actions. Instead, attack coordination was mostly delegated to the command-and-control servers of real botnets. This phase started on April 30 and lasted until May 18. It ran in four waves of different intensities, focusing on different targets and using different attack techniques. The "first wave" on May 4 included DDoS attacks on websites and DNS systems. Apart from that, the first week of May was relatively calm. The "second wave" on May 9-11 included DDoS attacks against mostly government websites and financial services. The "third wave" on May 15 included botnet-based DDoS attacks against government websites and financial industry. The "fourth wave" again consisted of attacks against governmental websites and banks.[38]

Among the most significant attacks during this second phase were the attacks on Hansabank. Estonia's largest bank, recently renamed to its parent company's name, Swedbank, owned a 50%

[36] Johnson, "Nokia Crisis Highlights Internal Struggle."

[37] Ironically, five years later, the response capacity based upon personal trust among the technical experts responsible for the Estonian ICT infrastructure possibly decreased, as some of experts had begun to operate from the headquarters of parent companies abroad.

[38] For a more detailed account on these "waves," cf. Tikk, *International Cyber Incidents*.

share of national retail banking, which is almost entirely Internet-based in web-savvy Estonia. Its lending volume in 2007 was close to 7.5 billion EUR, and its net profit in 2007 was 225 million EUR.[39] The web-interfaces for Internet-based services of the two biggest banks in Estonia were offline for about 45-90 minutes.[40] The downtime period and limited availability amounted to losses of about 1 million USD.[41] On May 10, a day after the attacks on Estonian systems had reached their highest intensity, Estonian news outlet Postimees reported that Hansabank was offline that morning, that customers would encounter problems throughout the day, and that customers from outside Estonia would be denied access to the webpage.[42]

Unlike the attacks in the first phase, the second phase relied on botnets, which are regarded as the main vehicle and platform for cyber-crime today. The construction and use of botnets is usually based on divisions of labor. Botnets are created by so-called “bot herders,” who often use malware kits created and sold by highly gifted programmers. “Bot herders” then either sell their botnets or rent them out for a certain span of time to other parties, who can then use the botnets to send out spam e-mail, distribute malware, or as in the Estonian case, launch DDoS attacks. The renting hours became visible from sharp rises of DDoS traffic at the beginning, and likewise steep falls at the end of a single attack.[43]

Technical Perspective of the Attacks

As noted before, the cyber attacks on Estonia did not resemble a single, ongoing, steady campaign, but consisted of a number of distinct attacks over the course of almost four weeks. In what constitutes one of the more detailed texts about the actual attack data and patterns, José Nazario, then a researcher at Arbor Networks (a vendor for Internet security solutions), blogged about dates, lengths, destinations, and bandwidths used during the attacks. Between May 3 and May 17, 128 unique DDoS attacks on Estonian websites were counted, of which "115 were ICMP floods, 4… TCP SYN floods, and 9… generic traffic floods."[44] The attacks were unevenly

[39] Hansabank Group, "Annual Report of Hansabank Group 2007."

[40] Ottis, "Conflicts in Cyberspace: Evgeny Morozov on Cyber Myths."

[41] Landler and Markoff, "In Estonia."

[42] "Hansapanka Tabas Küberrünne."

[43] Frankfurter Allgemeine Zeitung, "Estland Im Visler: Ist Ein Internetangriff Der Ernstfall?"; and Kaeo, "Cyber Attacks on Estonia: Short Synopsis."

[44] Nazario, *Estonian DDoS Attacks - A summary to date*.

distributed, with a mere three websites—the Ministry of Finance, the Police and Border Guard, and co-hosted websites of the Estonian government and the Prime Minister—being targeted in 106 of those 128 attacks.[45] Regarding the bandwidths used, 94 remained below 30 Megabits per second (Mbps), 22 were located in the range between 30 to 70 Mbps, and 12 were between 70 to 95 Mbps. Regarding the duration of distinct attacks, 31 of the attacks lasted more than one hour; of these, eight were between five to nine hours, and seven were more than ten hours. However, the most telling data on the effectiveness of the attacks is that "10 attacks measured at 90 Mbps, lasting upwards of 10 hours."[46]

This discussion of the Estonian cyber attacks might make one believe otherwise, but from a technical perspective, the thrust and sophistication of the attacks were relatively modest, if not low compared to global standards, even in 2007. A survey of ISPs in the US, Europe, and Asia on DDoS attacks conducted by anti-DDoS solution vendor Arbor Networks found: "In 2007, the largest observed sustained attack was 24 Gbps, compared to 17 Gbps in 2006. Thirty-six percent of the surveyed ISPs reported that they had observed attacks of over 1 Gbps in 2007."[47] In comparison, the Estonian attacks were modest.[48] Some interviewees from affected organisations even described the attacks and the effects on their systems as "boring." Given the overall capacity of the Estonian Internet, which was designed for a population of 1.4 million, these attacks were nevertheless suited to obstruct the Estonian Internet infrastructure.[49] In addition, the attacks lasted far longer than typical DDoS attacks—not just hours and days, but weeks, albeit interspersed with periods of no or little malicious traffic.[50]

Despite the lengthy duration, hiring a botnet to generate such malicious traffic would have been cheap. According to advertisements on Russian web forums, the costs to hire a botnet for DDoS

[45] *Ibid.*

[46] *Ibid.* Some Estonian experts doubt these figures, arguing that Arbor Networks could only see a fragment of the Estonian Internet and therefore underestimated the amount of malicious traffic.

[47] Arbor Networks, "Protecting IP Services from the Latest Trends in Botnet and DDoS Attacks," 2.

[48] Cf. Clover, "Kremlin-backed Group Behind Estonia Cyber Blitz."

[49] A presentation by Merike Kaeo, of doubleshotsecurity.com, provides some details on the topology of the Estonian Internet and government network. Kaeo, "Cyber Attacks on Estonia: Short Synopsis." The Estonian attacks showed that the low number and low capacity of international connections contributed to render Estonia's system unavailable. The connection of Georgian networks was even more poorly constructed, and therefore was less resilient to cyber attacks as the attacks in 2008 should prove.

[50] Marsan, "How Close Is World War 3.0? Examining the Reality of Cyberwar in Wake of Estonian Attacks."

services for 24 hours and a bandwidth of 100 Mbps was $75, and the price for a week of 1000 Mbps attacks was $600.[51] However, some security professionals involved in the response activities maintain that the attacks were technically and tactically more sophisticated, and required a larger group of knowledgeable persons.[52]

Countering DDoS

At the current stage of technology and legal developments, responding to a technical attack and mitigating DDoS attacks first and foremost requires the application of technical answers. Upscaling servers, offering a temporarily stripped down website, granting or denying access to the website to certain ranges of IP addresses, increasing bandwidth between targets and their ISPs or backbones, routing DDoS traffic to sinkholes—all of these techniques help to keep web services online.

A DDoS attack aimed at overstretching web server capacities can be countered by a reconfiguration of components on the network perimeter of an organization. For attacks flooding the network routes to an organization's infrastructure, a different defense approach is more promising: Malicious packets are dropped by conveying intermediaries located between the attacking and the attacked ends. This approach requires either administrative authority over the networks involved or collaboration with actors controlling parts of the Internet infrastructure that are conveying packets from the attacking systems to the target systems. Given today's ownership stucture, the Internet's network configurations, and the absence of central operational control, the only feasible option is globally distributed collaboration.

The second phase of attacks was based on botnets, with bot-infected drones scattered on machines located in numerous countries, emitting innumerable DDoS packets. The short-term response to such an attack is to apply some or any of the aforementioned mitigation techniques. If a botnet is operational for weeks and is dedicated solely to a specific DDoS attack, the defending actors would probably want to take down the botnet itself, e.g., by taking over its

[51] Segura and Lahuerta, "Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study", 114. A previous version of their article with identical figures was presented at the The Eighth Workshop on the Economics of Information Security in 2009; screenshots in that version of the article captured advertisements published in September 2008. (http://weis09.infosecon.net/files/113/index.html) It is therefore safe to assume that prices for DDoS services were not significantly higher at the time of the attacks.

[52] Interviews with the author.

command-and-control system. Takedowns of sophisticated botnets usually require months of investigation, research, and preparation. In addition, botnet surveillance was only in its infancy in 2007. Nevertheless, two Estonian interviewees from different governmental-administrative authorities stated that they had been able to indentify the persons responsible for the DDoS attacks and for providing the botnets used.[53]

International Collaboration

Once the attacks entered the second phase and became botnet-based, international collaboration and coordination became necessary. According to the Estonian Permanent Undersecretary of Defense, the Ministry of Defense was responsible for organizing international support,[54] mainly in the political sphere. This responsibility did not include the self-organized collaboration of operational teams and technical experts. With the Estonian government framing the DDoS attacks as a security issue caused by the Russian government, this attracted close attention from the Western media and governments.

On the international operational level, Estonian Internet security experts collaborated with the global Internet security operations community and CERTs in other countries, mainly in Finland (CERT-FI), Germany (CERTBund) and Slovenia (SI-CERT). CERT-EE, drowning in information and work during the response efforts and operating at the edge of, if not beyond its capacities, welcomed the help offered by their Finnish colleagues. The neighbours from the other side of the Baltic Sea analyzed, processed, and then disseminated attack telemetry data to the operators of those Internet segments, from which some of the attacks possibly originated.

The international collaboration included other contributors in addition to these distinct national CERTs, for they had no operational control over networks and systems in their home countries, nor did they have the staff for such operations. Thus, contributions to the response effort also came from a range of actors, including network companies, vendors of security appliances and network hardware, law enforcement and other security authorities, non-profit internet security organizations, and a number of individual ICT security professionals from Estonia, Russia, and other places around the world. These participants provided appliances, hardware, and more

[53] Interviews with the author.

[54] Kash, "Lessons From Cyberattack."

bandwidth; filtered malevolent traffic; or provided information necessary to understand the scope, nature, and technical details of the ongoing attacks. It is in the nature of these mailing-list based security communities that tasks emerging from security incidents are picked up by members according to a variety of factors. These include their role within their companies, their company's overall commercial interests, their personal interests, current workload, and their perceptions of the necessity and self-imposed responsibility to intervene. The lack of a central global Internet security monitoring facility, the distribution of situational knowledge, and the distribution of control over systems requires a loosely coupled networked approach. But it also requires a certain level of trust to share potentially delicate security information. The provider of such information shares details of apparantly compromised computers, while the receiver uses such data, for example, to block the Internet traffic of customers with allegedly compromised machines. In early May 2007, there was no deep trust between Estonian security experts on the one hand and the wider global security communities on the other. These are the groups that frequently deal with DDoS attacks on the Internet.

Good luck assisted with the rescue. The cooperation between the international and the Estonian communities was significantly facilitated by the attendance of contact persons at the annual meeting of TF-CSIRT in Prague on 3 May, an annual convention of invited European CERT security experts, and a long-planned RIPE meeting in Tallinn on 7 May.[55] It was at this RIPE meeting that members of the Estonian technical community were eventually introduced to members of the international technical Internet community. With the help of warrantors, who were trusted by the international community and vouched for the integrity of the Estonian newbies, the Estonian technical people were gauged as trustworthy. With this newly achieved status as members of the international technical community, a few Estonians could, for example, send lists with attacking IP addresses to mailing-list-based security communities such as NSP-

[55] The *Réseaux IP Européens Network Coordination Centre* is one of the five global Regional Internet Registries (RIRs) and provides "global Internet resources and related services (IPv4, IPv6 and AS Number resources) to members in the RIPE NCC service region" (http://www.ripe.net/lir-services/ncc). The region encompasses countries on the Eurasian landmass, minus those east of Iran and Kazakhstan.

Sec.[56] Network security professionals around the world that are members of such a list would then help to stop malicious traffic from flowing from their networks towards Estonian systems.

To summarize, the situation was mitigated by a range of technical measures. First, the capacities of the Estonian Internet services and the underlying systems were increased and scaled up. Second, filtering mechanisms were added to the structural layout of the Estonian Internet; these would drop malicious data packets before they would reach their targeted systems. Probably the most effective method was to block access and drop traffic to Estonian servers from outside the country. These measures made systems unavailable from abroad—a situation that was widely reported in the international press, but they also ensured the availability of web services and ICT-based services for the Estonians within the country. Traffic geographically originating from foreign countries was again routed to Estonian servers, once the ratio of benevolent to malevolent traffic was back to normal levels.[57]

Costs of the Attacks

The influx of DDoS packets had consequences on the quality and availability of Estonian web services—mainly regarding the loss of services for government, communication, and banking.[58] The e-mail and web services of some Estonian organizations were partly unavailable or functioned only at a reduced level. Government officials and journalists had difficulties obtaining access to their email accounts or the Internet.[59] As one would expect for non-physical attacks like DDoS, the information technology structure was left undamaged, but a “leading Estonian information technology expert” claimed that the attacks “were clearly aimed at destroying the Baltic country's Internet backbone.”[60] According to security professional and researcher José

[56] Bill Woodcock, networking professional, and co-founder and research director of Packet Clearing House, shared more details on the role of NSP-Sec in mitigating global DDoS attacks during a previous ACUS event. ACUS, “Building a Secure Cyber Future.” Kurtis Erik Lindquist from Swedish Internet Exchange Point operator Netnod, Woodcock, a third mediating person, and Hillar Aarelaid of CERT-EE established a trust-based collaboration between the Estonian technical community and a global community of network operators.

[57] Goodman, "Cyber Deterrence - Tougher in Theory Than in Practice?"

[58] Ashmore, "Impact of Alleged Russian Cyber Attacks," 4, 8.

[59] "Estonia Hit by Moscow Cyber War."

[60] Arnold, "Russian Group's Claims Reopen Debate on Estonian Cyberattacks." According to a person from Estonia’s cyber policy circles, the attackers managed to physically destroy a network component at an Estonian ISP.

Nazario, there have been “no apparent attempts to target national critical infrastructure other than Internet resources, and no extortion demands were made.”[61]

Despite the press coverage and the political attention that the attacks aroused, a comprehensive post-mortem with a listing of precise downtimes and times of reduced service, aggregated and grouped per organization, and complemented by a rough calculation of estimated financial consequences has yet to be written. The lack of data can be traced to the absence of overall monitoring of the Estonian Internet systems in 2007 and to the omission of systematic reporting by technical staff during the crisis. While the Estonian technical community still has an abundance of data and log files, which could provide these answers (Estonian language skill would be required to read this data), Estonian practitioners and international researchers alike obviously deemed such a study to be unimportant.[62] Existing anecdotical evidence of damages that occurred during the Estonian cyber attacks supports the conclusion that, despite shrill rhetoric heard during the course of the events and in the aftermath, the financial losses more likely were “minimal.”[63]According to Rain Ottis, “only a few critical on-line services (like banks) were affected for clients inside Estonia,” while “non-critical services (public government websites and news sites, for example) did suffer longer service outage.”[64]The costs of the response activities, however, haven't been mentioned anywhere in the existing literature. Nor have the expenses for new hardware to scale up existing systems or to harden the perimeters of corporate networks. Similarly, no cost figures have been issued for over-time work required of the operational staff. According to an interviewee close to Estonian government circles, some banks accumulated substantial opportunity costs created by lost revenues.[65] One company’s executive described the impact of delegating ICT staff to incident response tasks on ongoing ICT projects, and the necessity to both re-plan and re-organize these projects as the most

[61] "Estonian DDoS - a Final Analysis."

[62] During the review process of this chapter, sources close to the Estonian MoD informed me that the Estonian Ministry of Defence had indeed written such a report, which was soon to be declassified. There was insufficient time to incorporate that source in this chapter.

[63] Ashmore, "Impact of Alleged Russian Cyber Attacks," 8.

[64] Ottis, "Conflicts in Cyberspace."

[65] I have not interviewed risk managers or persons with similar roles in banks that could have backed up these claims.

prominent cost factors. Nevertheless, none of these costs should add up to figures creating greater public concern.

It is arguable whether the same can be said for the medium- and long-term effects of the relocation of the Bronze Soldier monument. The Estonian GDP numbers show solid, yet already decreasing GDP growth during the quarter of the attack. The trend of decreasing growth rates started several quarters before the attacks and continued afterwards into the financial crisis, sending the Estonian GDP into a brutal (-)14.1% nosedive in 2009, after an already displeasing previous year with a (-)3.6% recession.[66] The *Baltic Times* reported that Estonia's Transit sector income took a sharp hit in 2007, decreasing by 40% compared to the previous year. Russia, depending on ice-free Baltic harbors, has since diverted her cargo business from Tallinn's port to Latvia and Lithuania. According to an Estonian report and a Financial Ministry official mentioned in the article, Russia's economic payback aggregated to reductions in the Estonian GDP between 1 and 3.5 percent.[67] However, these reductions were for the Russian response as a whole and not just for the cyber attacks.

On the positive side, Estonia profited from a number of intangible and political gains. The attacks and the respective response turned Estonia into a household brand for all matters cybersecurity, which likely helped to secure the hosting of the NATO Cooperative Cyber Defense Center of Excellence and EU Agency for large-scale IT systems.[68] Its vanguard status was only increased by Estonia's provision of support in some international cyber-crime cases. Politically, Estonia managed to secure an increased commitment from NATO and the European Union, thereby advancing its strategic foreign policy goal of strengthening integration into Western institutions, which serve to balance the influence of neighboring Russia.[69] These issues lead to consideration of the international and geopolitical implications of the Estonian cyber attacks, which probably have been more influential than the effects on Estonian ICT systems.

[66] Cf. data provided by Statistics Estonia: Eesti Statistika, *Statistical Yearbook of Estonia 2009*, 26, and Eesti Statistika, *Statistical Yearbook of Estonia 2010*, 30.

[67] "Was It Worth It?"

[68] European Commission - DG Home Affairs, "What We Do - EU Agency for Large-scale IT Systems."

[69] On Estonia's foreign policy options and strategies: Danckworth, "Estlands Außenpolitik nach dem Beitritt zur Europäischen Union: Handlungsoptionen eines Kleinstaates." (Doctoral thesis on "Estonia's foreign policy after its accession to the European Union: Courses of action of a small state".)

The Politics of Cber Attacks

Soon after it had become obvious that problems with the Estonian Internet were caused by malevolent DDoS attacks, officials in Estonia started blaming Russian authorities for being behind it. Ene Ergma, President of the Riigikogu, the Estonian Parliament, likened the attacks to “a nuclear explosion;” the cyber attacks were “the same thing.” [70]The Estonian Minister of Justice asserted that some of the data packets in the flood were traced to IP addresses belonging to Moscow offices of the Kremlin.[71] Prime Minister Andrus Ansip blamed the Russian government directly.[72] In an interview with a German daily a good month after the attack, President Ilves used slightly more contained wording regarding the role of Russia. He avoided calling it warfare, but asked how to label such kinds of attacks and said, referring to the potential unavailability of emergency lines, that the attacks also “touched questions of life and death.” Furthermore, he referred to the fact that Russian computers were involved in the attacks, and that Russian intelligence service FSB would be able to control the Russian Internet.[73] Ilves also stated that some European states would have gone too far with their appeasement approach toward Russia.[74] Media representatives shared the view of Estonian incumbents. The editor of the Estonian *Postimees* newspaper and website, Merit Kopli, spoke decisively about the responsibilities: "The cyber attacks are from Russia. There is no question. It is political."[75]

The immediate assumption that Russian authorities were involved was soon expressed by Estonian officials, and subsequently by scholars[76] who studied the Estonian incident and interviewed Estonian officials in the months after the attacks. Other researchers have subsequently agreed with that assessment. Bumgarner and Borg emphatically blamed “Russia,” but they did not provide details about the specific role of the Russian authorities.[77] Healey stated,

[70] Poulsen, "‘Cyberwar’ and Estonia’s Panic Attack."

[71] Rantanen, "Virtual Harassment, but for Real."

[72] "Estonia Hit by Moscow Cyber War."

[73] Frankfurter Allgemeine Zeitung, "Estland Im Visier."

[74] NATO later revised its policy toward the Baltic states in 2009, after Germany dropped its resistance to including the Baltic states into NATO’s defense and contingency planning."US Embassy Cables: Germany Behind NATO Proposal for Baltic States."

[75] Thomson, "Russia 'hired Botnets' for Estonia Cyber-war.”

[76] E.g., Blank, "Web War I: Is Europe's First Information War a New Kind of War?"; and Grant, "Victory in Cyberspace."

[77] Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008." The full report of the US Cyber Consequences Unit has not been released publicly.

"the obvious truth: the attacks were supported or encouraged by the Russian government and… to make the attacks stop, Western decision makers needed to engage Moscow." [78]Ashmore's detailed account of Russia's role in the attacks concluded that an involvement of Russian authorities had not been proven, but the mere belief of Russian involvement continued to frame Russian-Estonian relations until today.[79] Evron's opinion was typical for a representative of the technical community,[80] and has been shared by many of the operational staff involved in the technical analysis and mitigation in interviews with the author. Evron was reserved about blaming the Russian government, given the lack of direct evidence and a smoking gun. In contrast to the rhetoric used by some politicians and cyberwarfare theorists, technical experts have shied away from calling the incident "cyber warfare."

Historiographic knowledge about the Russian policy during these events still is ambiguous and meagre. Gauging the involvement of the Russian government both in the attacks and their termination is difficult, given the lack of sound and first-hand sources, as Russia's governmental records of those months still have the Cyrillic version of the NOFORN stamp or higher. Lacking indisputable facts, assessments concerning Russia's role are therefore mainly based on perceptions of Russian foreign policy strategies, the weight of indications that Russia was involved, and the epistemological threshold that may be reached before pieces of circumstantial evidence add up to a picture "beyond reasonable doubt."

The assumptions concerning involvement by the Russian government and/or their close relationship to the unidentified perpetrators has been based on a number of arguments.[81] These include the arguments that Russian and Kremlin IP addresses were involved in the attacks;[82] that Russian experts had previously executed similar attacks using the same botnets;[83] that online and

[78] Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," 2.

[79] Ashmore, "Impact of Alleged Russian Cyber Attacks," 8.

[80] Evron, "Authoritatively, Who Was Behind the Estonian Attacks?"

[81] Partly compiled from Mützenich, "Nutzung Neuer Medien Als Instrument Russischer Außenpolitik," 8-9.

[82] "Estonian PM, Justice Minister Insist That Cyber Attacks Came From Kremlin Computers."

[83] Grant, "Victory in Cyberspace," 6.

offline protests were coordinated;[84] that the scale and sophistication of the attacks required a serious organization for coordination;[85] that the Kremlin-directed Nashi youth group was involved;[86] that the attacks required long-term planning;[87] that Russia possesses an asymmetric strategy that it employs against its increasingly West-leaning neighbors;[88] that Soviet and Lenin tactics were applied;[89] and that Russian law enforcement agencies did not cooperate with their Estonian counterparts .[90]

While these arguments carry some weight, they do not add up to evidence "beyond any doubt." The attacks did not have a serious, let alone long-term impact on the Estonian society. More decisive from a political perspective are the long-term implications of the viability and utility of

[84] Accoding to an interviewee from Estonia's non-technical security circles, some of the organizers of the offline riots had been paid for their services by Russian intelligence services. An IT executive stated that local Estonian-Russians had likely opposed the riots due to their probable negative impact on the Estonian economy, which would be against their personal interests. Interviews with the author. Nevertheless, the Russian minority was highly likely to join in public demonstrations, some of which were decentrally organised by snowballing text messages, which is akin to techniques that later became popoular in Iran or during the Arab Spring.

[85] An argument for sophistication, advanced by members of Estonian policy circles, is that the attacks focused on a "key network device" in Estonia's internet infrastructure. The attackers had required detailed knowledge of the Estonian infrastructure, and the attacks resembled a "power demonstration of what can be done." One Estonian security professional described them as "targeted, single-packet router-killing stuff, never seen before." Another dryly stated that there still was the possibility of pure chance that a router and its replacement got broken in quick succession. In addition, some hardware components are known to be vulnerable to so called "Packets of Death." Another example of sophistication that was mentioned was a sample of a bot malware, which foreign security experts and police forces managed to obtain on behalf of the Estonian CERT. However, International malware experts told me that bot malware involved in the attacks was "not far beyond what had already been detected in the wild" back in 2007. All quotes from different interviews with the author.

[86] Evron, "Who Was Behind"; Grant, "Victory in Cyberspace," 6; and Ashmore, "Impact of Alleged Russian Cyber Attacks," 25.

[87] Interviewees from Estonian policy circles stated that the first signs of the attacks appeared long before the attacks themselves; among these signs were very brief, intense floods of data packages designed to measure the capacity of the Estonian ICT infrastructure. The time span appears to have been interpreted as an indication of strategic long-term planning by Russian authorities, and serves as a counter-argument to the thesis of spontaneous online-riots that is advanced by Russian nationalist "geeks."

[88] Blank, "Web War I," 230.

[89] *Ibid*., 230.

[90] Evron, "Battling Botnets," 124; and "Venemaa Keeldub Endiselt Koostööst Küberrünnakute Uurimisel." Estonian authorities handed over a list of Russian suspects deemed responsible for the cyber attacks (an interviewee from Estonian policy circles said: "We knew all the names of the criminals, we knew the masters"), and demanded their extradition based on the Estonian-Russian mutual extradition treaty. The request was rejected by Russian authorities. An IT staff member of an Estonian company stated that they had identified the "botmasters" and those "who organized these attacks," and that this information was then passed to the police. But unlike many other cases of cyber crime, the names of the suspects have never been publicized. Accoding to an interviewee, Estonian authorities preferred this affair to remain low-key. Interviews with the author.

such cyber attacks. The cyber attacks would have fit into Russia's overall foreign policy strategy toward its neighboring countries. Partly because of substantial ethnic Russian diasporas and partly because of security or national interests, Russia seeks to exert influence over the former satellite states that it had annexed in and after WWII and which gained their independence after 1991. Its foreign policy strategy has aimed at containing both Western influence in its neighboring countries and the advance of NATO facilities toward the Russian border.[91]

What could Russia have gained by the attacks? The actual consequences of the attacks have been rather mild because of the existence of an Estonian cybersecurity community, and because of its ability to timely link up to cybersecurity communities in neighboring European countries and around the world. If these communities hadn't been in place, things might have turned out differently. Given the still predominant ignorance surrounding the role of global technical communities in Internet security and incident response among Western cyber security pundits, it is save to assume that the attackers had not been aware of Estonia's response capabilities.

Without these capabilities, domestic politics would have been shaken up in Estonia. Had the attacks been successful, public and economic life in Estonia would have come to a standstill for days. After some time, probably a day or two, the technical experts would have discovered what to do, how, whom to collaborate with, and how to mitigate the DDoS attacks to bring ICT systems back to life. Much of the blame might have been placed on the Estonian incumbent, for his irreconcilable monument policy. His allegedly more Russia-friendly opponent, one of whose electoral strongholds resided in the Russian minority and who favored a more diplomatic approach to the war memorial problem, might have gained a more favorable image among the Estonian electorate. Presumably more important than such an immediate gain would have been the long term effects. A successful attack would have left the impression among Estonians that Russia is capable of encroaching on Estonian ICT systems and politics, if Russia feels fundamentally challenged by its neighbor's policies. Such an impression can lead to self-limitations in policy options; Russia would have increased its influence on one of the "near foreign countries."

[91] Mützenich, "Nutzung Neuer Medien Als Instrument."

From a political perspective, the strongest arguments for at least the remote involvement of Russian authorities relate to the overall Russian strategy regarding their neighboring countries, and the tactics applied to decrease their neighbors' collaboration with and leaning towards the West. However, no gains associated with these factors materialized during or after the attacks. Thus, whether the Russian government actually played a role in the attacks is a lesser question. The political lesson is that cyber attacks can potentially be used as an instrument to influence your neighbors domestic politics.

Conclusion

The attacks on the Estonian Internet infrastructure had only a relatively mild direct impact on Estonian society. Certainly, Estonian organizations and their IT deparments bore the costs of delegating their staff to handle incident reponse tasks, and political institutions' cultural capital was diminished by web defacements and other forms of ridicule. But the long-term relevance of the Estonian cyber attacks in 2007 is not that they allegedly constituted the first instance of an cyber war. This was not a war when one applies a serious and sober definition of that term. Yet, the attacks were a watershed event in the history of Internet security for two reasons.

First, the attacks made it seem plausible to a wider public that cyber attacks can be used as a tool in international or bilateral conflicts. This feature is demonstrable irrespective of how one answers the question of who was behind the attacks—whether it was a loosely-connected, *ad hoc* group of feverish Russian nationalist with varying (from little to über-geeky) degrees of IT skills plus some knowledge of how the cyber-crime underground economy works; or whether it was a team within the Russian FSB collaborating with befriended cyber-criminals of the Russian underground economy, connected with unknown levels up the ladder in Russia's security bureaucracy and administration. Irrespective of the answer, the attacks fitted well into the overall Russian foreign policy strategy developed to influence their neighboring countries at that time. This was characterized by an increasingly hard-line stance of the Kremlin and the drive to increase their cultural, political, and economic influence in countries neighbouring Russia's western borders.

The Estonian political response, in concert with their Western allies, was to deter Russia and other countries from attempting future applications of attacks against civil Internet infrastructure in another country. A mix of diverse policy approaches has been implemented. Government representatives have rushed to name-and-shame state-funded or state-tolerated attacks on civil ICT infrastructures, branding this sort of action illigitimate international conduct. Media coverage of the events has emphasized Russia's more dominant foreign policy in the nearer countries to Russia's borders, and has exposed close relationships between Russia's underground economy, intelligence services, and government circles. A long-term endeavour has been to shrink the "grey zone" of arguably just-barely-legal aggressive cyber-conduct. On the technical-operational side, increased alertness and preparedness for such attacks has been a goal of policy makers ever since.

Estonia and its Western security allies have assured their mutual support in the event of future, large-scale attacks on their ICT infrastructures, thereby raising the risks and potential costs for an adversary that tolerates or even utilizes voluntary groups to attack foreign Internet infrastructures. As a result, Estonia has become more embedded than ever into Western security and policy institutions, while Russia's cultural and political influence on Estonia has been further reduced. Whatever Russia's foreign policy circles had defined as strategic goals (if they were involved at all), the Estonian cyberattacks hardly advanced Russia's political causes.

The second reason is less obvious, but nonetheless highly relevant both for future Internet security incidents and regarding questions of democractic governance of communicational infrastructures. This involves the relationship between networks and hierarchies, between operators and owners of communicational infrastructures and traditional security institutions.

The Estonian cyber attacks will go down in history as a rare case in which a Minister of Defence stated that his country was in a "national security situation"—and yet the relevant contribution to straighten out the situation did not come from military staff, but from a community of technical experts, who cooperated in the settings of the "beer & sauna protocol" and fancy conferences that started at 2 pm with a morning pint, and who possessed values favoring effectiveness over procedure and protocol. The response to the Estonian attacks was a wild success for the technical security communities' principles of loose governance, trust-based information-sharing, and technology-facilitated *ad hoc* collaboration. At the same time, however, this marked the end of the community's autonomy from state interference and regulation. The relations between the domestic security community and the political sphere in more recent times are aptly symbolized by the locations of briefings for high-level politicians by the security community: they frequently take place in the offices of the Estonian CERT.

Cultural and communication conflicts between the technical community and the political sphere had already emerged during the attacks. Pieces of seemingly contradictory information from different sources of the community added up to an unclear picture of what was going on. Political boards became, at least temporarily, suspicious of information they received from the security community. As a thoughtfull member of the technical community put it, “Governments and institutions simply do not know how to communicate with the community. They do not know how to do it. They are not used to it.” And therefore, according to another member, “the biggest problem we face in these events is communication between hierarchies and networks.”[92] As a consequence, the community was formalized as a legal body (the Cyber Defense League); also, the informal core group of the response team now acts as a formalized technicial advisory body to Estonia’s National Security Council; and the CERT’s hosting organisation, RIA, has been granted special executive rights for future national security situations.

In an ideal world, such institutionalisation of the technical security communities helps to achieve two goals: to increase democratic control of Internet security governance, and to increase the capacities and abilities of the overall response organisation so that they may successfully counter hostile intruders. Time will tell whether these approaches will serve the Estonian and other societies well, or even better than the self-organized response of technical security communities in 2007.

Bibliography

Hillar Aarelaid, "Overview of Recent Incidents" (Presentation given at ENISA/ CERT CC Workshop on Mitigation of Massive Cyberattacks 19th September in Porto, Portugal) (September 19, 2007), http://www.enisa.europa.eu/act/cert/events/files/ENISA_overview_of_recent_incidents_Aareleid.pdf (accessed November 8, 2010).

[92] Quotes from interviews with the author.

Joe Alas, "May 9 Protestors Call for Removing Bronze Soldier Statue ", *Baltic Times* (May 10, 2006). http://www.baltictimes.com/news/articles/15345/.

Joe Alas, "Reformists Pull Off Surprise Victory, Consider Dumping Centrists", *Baltic Times* (March 7, 2007). http://www.baltictimes.com/news/articles/17358/ (accessed October 15, 2012).

Joe Alas, "Soldier Fails to Sway Elections", *Baltic Times* (February 21, 2007). http://www.baltictimes.com/news/articles/17358/ (accessed October 15, 2012).

Chloe Arnold, "Russian Group's Claims Reopen Debate on Estonian Cyberattacks", *Radio Free Europe / Radio Liberty* (2009). http://www.rferl.org/articleprintview/1564694.html.

Arbor Networks, "Protecting IP Services from the Latest Trends in Botnet and DDoS Attacks" (White Paper, 2009), 2.

William C Ashmore, "Impact of Alleged Russian Cyber Attacks", *Baltic Security & Defence Review* 11 (2009): 4-40. http://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf.

Risto Berendson, "Küberrünnakute Taga Seisavad Profid", *Postimees* (May 3, 2007), http://www.tarbija24.ee/120507/esileht/siseuudised/258409.php.

Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?", *Comparative Strategy* 27, no. 3 (2008): doi:10.1080/01495930802185312. Rebecca Grant, "Victory in Cyberspace" (Special Report, Air Force Association, October, 2007).

John Bumgarner and Scott Borg, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008" (*US-CCU Special Report*, U.S. Cyber Consequences Unit, August, 2009).

Cp. Charles Clover, "Kremlin-backed Group Behind Estonia Cyber Blitz", *Financial Times* (2009). http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?nlcick_check=l.

Till-Gneomar Danckworth, "Estlands Außenpolitik nach dem Beitritt zur Europäischen Union: Handlungsoptionen eines Kleinstaates" (Dissertation zur Erlangung des akademischen Grades doctor philosophiae (Dr. phil.) vorgelegt der Philosophischen Fakultät der Technischen Universität Chemnitz, 2007).

Eesti Statistika, *Eesti statistika aastaraamat 2009 ¬- Statistical Yearbook of Estonia* (July, 2009), Tallinn, http://www.stat.ee/31366 (accessed January 23, 2013).

Eesti Statistika, *Eesti statistika aastaraamat 2010 ¬- Statistical Yearbook of Estonia* (July 2010), Tallinn, http://www.stat.ee/38050 (accessed January 23, 2013).

"Estonian DDoS - a Final Analysis", *The H Security* (2007). http://www.h-online.com/security/news/item/Estonian-DDoS-a-final-analysis-732971.html.

"Estonian PM, Justice Minister Insist That Cyber Attacks Came From Kremlin Computers", *Baltic Times* (June 8, 2007). http://www.baltictimes.com/news/articles/18038

"Estonia Hit by Moscow Cyber War", *BBC News* (2007). http://news.bbc.co.uk/2/hi/europe/6665145.stm.

European Commission - DG Home Affairs, "What We Do - EU Agency for Large-scale IT Systems", http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/index_en.htm (accessed October 17, 2012).

Gadi Evron, "Authoritatively, Who Was Behind the Estonian Attacks?", *Dark Reading* (2009). http://www.darkreading.com/security/news/227700882/authoritatively-who-was-behind-the-estonian-attacks.html.

Gadi Evron and Hilar Aarelaid, "Estonia: Information Warfare and Lessons Learned" (Presentation given at the Workshop on Learning from large scale attacks on the Internet - Policy Implications, January 17, 2008).

Gadi Evron, "Battling Botnets and Online Mobs. Estonia's Defence Efforts During the Internet War", *Georgetown Journal of International Affairs* 9, no. 1 (2008): 121-126.

http://ec.europa.eu/information_society/policy/nis/docs/largescaleattacksdocs/s5_gadi_evron.pdf

”Gadi Evron, “[NANOG] An account of the Estonian Internet War, ge@linuxbox.org, 20 May 2008, http://mailman.nanog.org/pipermail/nanog/2008-May/000676.html (accessed January 2011)

Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic", *Washington Post* (May 19, 2007), http://www.washingtonpost.com/wp-dyn.content/article/2007/05/18/AR2007051802122.html.

Frankfurter Allgemeine Zeitung, "Estland Im Visler: Ist Ein Internetangriff Der Ernstfall?" (June 18, 2007). http://www.faz.net/s/RubDDBDABB9457A437BAA85A49C26FB23A0/Doc~E7CCF88CEFB6F467BB8D75A400C07B959~ATpl~Ecommon~Scontent.html (accessed November 4, 2010).

Hansabank Group, "Annual Report of Hansabank Group 2007" (2008).

"Hansapanka Tabas Küberrünne", *Postimees* (May 10, 2007). http://www.tarbija24.ee/180507/esileht/majandus/259920.php.

Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks", *Atlantic Council IssueBrief* (January, 2012), http://www.acus.org/publication/beyond-attribution-seeking-national-responsibility-cyberspace, 2.

"Here We Go Again", *Baltic Times* (April 4, 2007). http://www.baltictimes.com/news/articles/17635/.

Geoffrey A. Hosking, *Rulers and Victims--The Russians in the Soviet Union* (2006), Belknap Press of Harvard University Press, Cambridge, Mass.

Mikko Hyppönen, "Unrest in Estonia", *F-Secure Weblog* (April 28, 2007), http://www.f-secure.com/weblog/archives/00001181.html.

Mikko Hyppönen, "Update on the Estonian DDoS Attacks", *F-Secure Weblog* (April 30, 2007). http://f-secure.com/weblog/archives/00001183.html.

Bobby Johnson, "Nokia Crisis Highlights Internal Struggle", *BBC* (February 10, 2011). http://www.bbc.com/news/technology-12414595 (accessed February 10, 2011).

Wyatt Kash, "Lessons From the Cyberattack on Estonia. Interview with Lauri Almann, Estonia's Permanent Undersecretary of Defence", *Government Computer News* (June 13, 2008), http://gcn.com/Articles/2008/06/13/Lauri-Almann--Lessons-from-the-cyberattacks-on-Estonia.aspx?p=1.

Merike Kaeo, "Cyber Attacks on Estonia: Short Synopsis" (2007). http://doubleshotsecurity.com/pdf/NANOG-eesti.pdf.

Ian Kershaw, *Hitler, 1936-1945* (2000), Aus dem Englischen von Klaus Kochmann, 3. Auflage, Deutsche Verlags-Anstalt, Stuttgart.

Konstatin Kosachev, "An Insult to Our War Dead", *The Guardian* (March 6, 2007). http://www.guardian.co.uk/commentisfree/2007/mar/06/comment.second-worldwar.

Carolyn Duffy Marsan, "How Close Is World War 3.0? Examining the Reality of Cyberwar in Wake of Estonian Attacks", *Network World* (August 22, 2007). http://www.networkworld.com/news/2007/082207-cyberwar.html.

Robert A Miller and Daniel T Kuehl, "Cyberspace and the 'First Battle' in 21st-century War" (National Defense University, Center for Technology and National Security Policy, 2009), 3.

Rolf Mützenich, "Die Nutzung Neuer Medien Als Instrument Russischer Außenpolitik in Seinem „Nahen Ausland“, *Website of German MP R. Mützenich* (2009), http://www.rolfmuetzenich.de/texte_und_reden/veroeffentlichungen/Muetzenich_SF.pdf.

Stephen Lee Myers, "Debate Renewed: Did Moscow Free Estonia or Occupy It?", *New York Times* (January 25, 2007). http://www.nytimes.com/2007/01/25/world/europe/25tallinn.html.

"NATO Sees Recent Cyber Attacks on Estonia As Security Issue", *DW-World* (May 26, 2007). http://www.dw.de/nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579.

Kevin Poulsen, "'Cyberwar' and Estonia's Panic Attack", *Wired, Threat Level* (August 22, 2007), http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/ (accessed November 10, 2010).

José Nazario, "Estonian DDoS Attacks - A summary to date", Arbor Networks, (May 17, 2007), http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

Nerious Adomaitis, "Estonia Calm After Red Army Site Riots, Russia Angry", *Reuters* (April 28, 2007). http://www.reuters.com/article/2007/04/28/us-estonia-russia-idUSL2873034620070428/ (accessed October 15, 2012).

Rain Ottis, "Conflicts in Cyberspace: Evgeny Morozov on Cyber Myths" , Web (June 26, 2009), http://conflictsincyberspace.blogspot.com/2009/06/evgeny-morozov-on-cyber-myths.html (accessed December 12, 2011, confirmed by Estonian interviewees)

Tamo Randel, "CyberWar in Estonia 2007 - History, Analysis" (Presentation given at IMPACT 2008, Malaysia) (2008), http://www.impact-alliance.org/downloads/TarmoRandel_CyberwarInEstonia.pdf.

Miiska Rantanen, "Virtual Harassment, but for Real", *Helsingin Sanomat International Edition* (May 6, 2007). http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868.

Iain Thomson, "Russia 'hired Botnets' for Estonia Cyber-war - Russian Authorities Accused of Collusion with Botnet Owners", *Computing.co.uk* (May 31, 2007). http://www.computing.co.uk/vnunet/news/2191082/claims-russia-hired-botnets.

V Segura and J Lahuerta, "Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study," in *Economics of Information Security and Privacy*, ed. Tyler Moore, David J Pym and Christos Ioannidis (New York et al. : Springer, 2010), 114.

Richard Sietmann, "22C3: Pro Und Kontra E-Voting", *heise online* (December 29, 2005). http://www.heise.de/newsticker/meldung/22C3-Pro-und-Kontra-e-Voting-161678.html (accessed January 15, 2011).

Vladimir Socor, "Moscow Stung by Estonian Ban on Totalitarianism's Symbols", *Eurasia Daily Monitor, The Jamestown Foundation* (January 26, 2007). http://jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=32427.

"US Embassy Cables: Germany Behind NATO Proposal for Baltic States", *The Guardian* (December 6, 2010). http://www.guardian.co.uk/world/us-embassy-cables-documents/240187.

Will Goodman, "Cyber Deterrence - Tougher in Theory Than in Practice?", *Strategic Studies* 102 (2010).

"Was It Worth It?", *Baltic Times* (May 1, 2008). http://www.baltictimes.com/news/articles/20360/ (accessed October 23, 2012).