The Estonian Cyberattacks

Andreas Schmidt[1]

For three weeks from 27 April until 18 May 2007,[2] components of the Estonian Internet infrastructure were subjugated to Distributed Denial of Service (DDoS) attacks, massive e-mail and comment spam, website defacements, and DNS server attacks. 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 an ideologically motivated minority of predominantly ethnic Russians on the other. As a result, 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.

This chapter offers a descriptive account of the attacks, the damages that they inflicted, and the responses made. The 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 1947, when major affairs in the Estonian Socialist Soviet Republic were controlled from Stalin's Kremlin, the "Monument to the Liberators of Tallinn" 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.[3] 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

1 Andreas Schmidt is a researcher at the Faculty of Technology, Policy, and Management at Delft University of Technology. He holds a Masters degree in Political Science and Medieval and Contemporary History. He is currently writing his Ph.D. thesis on the role of technical communities in Internet security governance.

2 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.

3 Hosking, Rulers and Victims, 206.

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,[4] 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 2005.[5]

Unsurprisingly, the monument emerged as the site where different interpretations of the role of the Red Army were expressed in demonstrations.

It didn't go unnoticed in Moscow that its former Soviet republic was about to cut ties with 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 prevent the statue from being moved. On 3 April, 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.[6] The conflict was about Estonian identity, relations between Russia and Estonia, and the perception of World War II.[7] 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.[8] In the eyes of (some) 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.[9]

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 4 March 2007. "War graves are no place for day-to-day politics," warned President Toomas Hendrik Ilves, a Social Democrat, but to no avail.[10] 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.[11] The elections confirmed the Prime Minister's new term, and the Reform Party finished ahead of the

4 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.

5 Alas, "May 9 Protestors Call for Removing Bronze Soldier Statue."

6 "Here We Go Again."

7 Myers, "Debate Renewed: Did Moscow Free Estonia or Occupy It?"

8 Kosachev, "An Insult to Our War Dead."

9 Socor, "Moscow Stung by Estonian Ban on Totalitarianism's Symbols."

10 Alas, "Soldier Fails to Sway Elections."

11 *Ibid.*

social-liberal Center Party and its candidate, who preferred a less controversial approach regarding the monument.[12] In March, Ansip's new government immediately laid the legal ground for the removal of the Bronze Soldier.

On 26 April, Estonian authorities fenced off the statue in the center of Tallinn. A day later, they removed the statue, and after several weeks exhumed bodies of Red Army soldiers that had been buried near by, any unclimed remains were transferred to a military cemetery in Tallinn a few kilometers away.[13] 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, the streets were filled with protesters, rallying against the decision of the Estonian government. Estonian police forces arrested hundreds of protesters.[14] In the late evening of the day of the monument's removal, on Friday, 27 April,[15] 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.[16]

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

Political institutions were early targets of the attacks. Estonian Prime Minister Andrus Ansip and other leading politicians were spammed.[17] The email services of the Estonian parliament had to be temporarily shut down, as they were no longer able to handle the

12 Alas, "Reformists Pull Off Surprise Victory, Consider Dumping Centrists."
13 "NATO Sees Recent Cyber Attacks on Estonia As Security Issue."
14 Adomaitis, "Estonia Calm After Red Army Site Riots, Russia Angry."
15 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 this, traffic first abnormally increased on Friday night around 10:15 pm, but culminated no earlier than late Sunday, April 28. Interviewees confirmed that attacks started on a Friday, i.e., on April 27.
16 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."
17 Berendson, "Küberrünnakute Taga Seisavad Profid."

unusual data payload.[18] 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.[19] 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."[20]

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 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 ten, resulting in malfunctions or non-availability of Internet services.[21] 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 28 April. 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 eight-four of 166 cases until Monday early morning.[22] 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).[23]

Boot-up of the Estonian Response

18 Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic."
19 "Hansapanka Tabas Küberrünne."
20 Berendson, "Küberrünnakute."
21 Aarelaid, "Overview of Recent Incidents."
22 Hyppönen, "Update on the Estonian DDoS Attacks."
23 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), said 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." See also 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.

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 shared by many in the Estonian security community.[24] But it wasn't only intuition which led to the expectation that some sort of cyberattacks were coming. The message was spreading within both Estonian and international Internet security communities in mid-April that commenters were calling within Russian-language forums for a 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.[25]

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 starting to protect the Estonian national critical infrastructure."[26] Not much later, Estonia's informal ICT security community linked up with traditional security institutions. 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 national election sites. Exposing the vulnerabilities of electronic voting systems had become a favorite pastime among hackers worldwide, an

24 Estonian ICT security expert interviewed by the author. Empirical findings in this chapter are, aside from 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), and their ability to provide additional explanations of technological, organizational, or political circumstances. Most interviewees worked as security professionals in organizations 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 due to previous press coverage. The interviews for the Estonian case were conducted in 2011 and 2012 during research trips to Estonia, California, and various other places in Europe, usually for Internet (security) conferences such as the Internet Governance Forum, TF-CSIRT, GovCERT NL, and FIRST meetings, and also for closed gatherings of the Internet security community. In 2013, I had a few additional background conversations or follow-up interviews.

25 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. Priisalu, "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. Apparently, 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.

26 An Estonian interviewee.

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.[27] The task force tried to reduce these risks by continuously monitoring 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 8 May to be the most likely date for a spill-over of the offsite riots to the digital sphere: "We had everything ready."[28] 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. In Russia, web forums publichsed descriptions of how to harm Estonian servers, along with respective Windows command shell scripts and pleas to run those scripts at a certain point of time.[29] Thousands of people running these scripts simultaneously can cause 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.

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.

Four hours after the attacks had commenced, at 2 am in the early morning of Friday, 27 April, operational teams responsible for governmental servers had realized from mutual updates by telephone that some government websites were being exposed to Internet traffic exceeding normal traffic by 100 to 1,000 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.[30] 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 28 April, "We are under cyberattack."[31] His superior, the Estonian Minster

27 Sietmann, "22C3: Pro und Kontra e-Voting."

28 An Estonian interviewee.

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

30 Evron and Aarelaid, "Estonia."

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

of Defense Jaak Aaviksso said, "It turned out to be a national security situation."[32]

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."[33] Hillar Aarelaid, one of the then two full-time staff-members and head of CERT-EE,[34] 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]."[35] The most significant role in the technical response activities certainly was handled by the Estonian CERT.[36]

The most significant role in the technical response activities certainly was handled by the Estonian CERT.

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,[37] 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.[38] On 30 April, Estonian experts came together for a joint meeting, representing organizations

The "beer & sauna protocol" helped to formulate a degree of trust among the Estonian experts that allowed them to collaborate seamlessly during the attacks.

32 Landler and Markoff, "In Estonia."
33 Kash, "Lessons From Cyberattack."
34 Randel, "CyberWar in Estonia 2007 - History, Analysis."
35 Aarelaid, "Overview."
36 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 criticized the centrality of CERT-EE, as that had established a single-point of failure in the Estonian response. This organizational vulnerability could have been exploited by the attackers.
37 Johnson, "Nokia Crisis Highlights Internal Struggle."
38 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 the experts had begun to operate from the headquarters of parent companies abroad.

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 30 April and lasted until 18 May. It ran in four waves of different intensities, focusing on different targets and using different attack techniques. The "first wave" on 4 May included DDoS attacks on websites and DNS systems. Apart from that, the first week of May was relatively calm. The "second wave" on 9-11 May included DDoS attacks against mostly government websites and financial services. The "third wave" on 15 May included botnet-based DDoS attacks against government websites and the financial industry. The "fourth wave" again consisted of attacks against governmental websites and banks.[39]

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 percent 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.[40] The web-interfaces for Internet-based services of the two biggest banks in Estonia were offline for about 45-90 minutes.[41] The downtime period and limited availability amounted to losses of about one million USD.[42] On 10 May, 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.[43]

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

39 For a more detailed account on these "waves," cf. Tikk, et al, "International Cyber Incidents."
40 Hansabank Group, "Annual Report of Hansabank Group 2007."
41 Ottis, "Conflicts in Cyberspace: Evgeny Morozov on Cyber Myths."
42 Landler and Markoff, "In Estonia."
43 "Hansapanka Tabas Küberrünne."

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.[44]

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, is a long form blog post by José Nazario, then a researcher at Arbor Networks (a vendor for Internet security solutions). Between 3 May and 17 May, 128 unique DDoS attacks on Estonian websites were counted, of which "115 were ICMP floods, four... TCP SYN floods, and nine... generic traffic floods."[45] The attacks were unevenly 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. Regarding the bandwidths used, twenty-two were located in the range between thirty to seventy Mbps, and twelve were between seventy to ninety-five Mbps. Regarding the duration of distinct attacks, thirty-one of the attacks lasted more than one hour; of these, seven lasted more than ten hours. However, the most telling data on the effectiveness of the attacks is that "10 attacks measured at ninety Mbps, lasting upwards of ten hours."[46] Unfortunately, these local sensors did not catch attacks directed against the banks, which according to Jaan Priisalu, then Head of IT Risk Management at Hansabank, were far more severe having dynamically filled all available chanels and having crested at 3gbps. One botnet that targeted Hansabank was comprised of 82,000 machines.[47]

From a technical perspective, the thrust and sophistication of the attacks directed against government websites was 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 Arbor Networks found: "In 2007, the largest observed sustained attack was twenty-four Gbps, compared to seventeen Gbps in 2006. Thirty-six percent of the surveyed ISPs reported that they had observed attacks of over one Gbps in 2007."[48] In comparison, the Estonian attacks were modest.[49] Some interviewees from affected organizations 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.[50] In addition, the

44 Frankfurter Allgemeine Zeitung, "Estland Im Visier: Ist Ein Internetangriff Der Ernstfall?"; and Kaeo, "Cyber Attacks on Estonia: Short Synopsis."
45 Nazario, "Estonian DDoS Attacks - A summary to date."
46 *Ibid.*
47 Details from Hansabank come from an email forwarded by Luukas Kristjan Ilves detailing notes by Jaan Priisalu.
48 Arbor Networks, Protecting IP Services from the Latest Trends in Botnet and DDoS Attacks, 2.
49 Clover, "Kremlin-backed Group Behind Estonia Cyber Blitz."
50 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.

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.[51]

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 services for twenty-four hours and a bandwidth of 100 Mbps was $75, and the price for a week of 1000 Mbps attacks was $600.[52] 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.[53]

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 structure, 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

51 Marsan, "How Close Is World War 3.0? Examining the Reality of Cyberwar in Wake of Estonian Attacks."
52 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.
53 Interviews with the author.

attack, the defending actors would probably want to take down the botnet itself, e.g., by taking over its 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 identify the persons responsible for the DDoS attacks and for providing the botnets used.[54]

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,[55] 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 neighbors 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 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

54 Interviews with the author.
55 Kash, "Lessons From Cyberattack."

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 apparently 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.[56] 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-SEC.[57] 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

56 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.
57 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. Woodcock, "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.

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.[58]

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.[59] 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 web services, like email, which inhibited basic administrative actions like sending out a press release .[60] 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."[61] According to security professional and researcher José Nazario, there have been "no apparent attempts to target national critical infrastructure other than Internet resources, and no extortion demands were made."[62]

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.[63] Existing anecdotal 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."[64] 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

58 Goodman, "Cyber Deterrence - Tougher in Theory Than in Practice?"
59 Ashmore, "Impact of Alleged Russian Cyber Attacks," 4, 8.
60 "Estonia Hit by Moscow Cyber War."
61 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.
62 "Estonian DDoS - a Final Analysis."
63 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.
64 Ashmore, "Impact of Alleged Russian Cyber Attacks," 8.

news sites, for example) did suffer longer service outage."[65] 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.[66] 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 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 stayed solid during the quarter of the attack, continuing a slow recession that lasted until the Estonian GDP had a brutal (-)14.1 percent nosedive in 2009 .[67] While a small sector of the national economy, the *Baltic Times* reported that Estonia's Transit sector took a sharp hit in 2007, decreasing by 40 percent 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.[68] 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.[69] 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.[70] These issues lead to consideration of the international and geopolitical implications of the Estonian cyber attacks, which probably have been more

65 Ottis, "Conflicts in Cyberspace."
66 I have not interviewed risk managers or persons with similar roles in banks that could have backed up these claims.
67 Cf. data provided by Statistics Estonia: Eesti Statistika, Statistical Yearbook of Estonia 2009, 26, and Eesti Statistika, Statistical Yearbook of Estonia 2010, 30.
68 "Was It Worth It?"
69 "What We Do - EU Agency for Large-scale IT Systems."
70 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".)

influential than the effects on Estonian ICT systems.

The Politics of Cyber 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."[71] 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.[72] Prime Minister Andrus Ansip blamed the Russian government directly.[73] 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.[74] Ilves also stated that some European states would have gone too far with their appeasement approach toward Russia.[75] 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."[76]

The immediate assumption that Russian authorities were involved was soon expressed by Estonian officials, and subsequently by scholars[77] 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.[78] Healey stated, "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."[79] 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

71 Poulsen, "'Cyberwar' and Estonia's Panic Attack."
72 Rantanen, "Virtual Harassment, but for Real."
73 "Estonia Hit by Moscow Cyber War."
74 "Estland Im Visier."
75 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."
76 Thomson, "Russia 'hired Botnets' for Estonia Cyber-war."
77 E.g., Blank, "Web War I: Is Europe's First Information War a New Kind of War?"; and Grant, "Victory in Cyberspace."
78 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.
79 Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," 2.

belief of Russian involvement continues to frame Russian-Estonian relations until today.[80] Evron's opinion was typical for a representative of the technical community,[81] 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."

Historic knowledge of Russian policy during these events remains ambiguous and meager. 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.[82] These include the arguments that Russian and Kremlin IP addresses were involved in the attacks;[83] that Russian experts had previously executed similar attacks using the same botnets;[84] that online and offline protests were coordinated;[85] that the scale and sophistication of the attacks required a serious organization for coordination;[86] that the Kremlin-directed Nashi youth group was involved;[87] that the attacks required long-

80 Ashmore, "Impact of Alleged Russian Cyber Attacks," 8.
81 Evron, "Authoritatively, Who Was Behind the Estonian Attacks?"
82 Partly compiled from Mützenich, "Nutzung Neuer Medien Als Instrument Russischer Außenpolitik," 8-9.
83 "Estonian PM, Justice Minister Insist That Cyber Attacks Came From Kremlin Computers."
84 Grant, "Victory in Cyberspace," 6.
85 According 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 organized by snowballing text messages, which is akin to techniques that later became popular in Iran or during the Arab Spring.
86 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.
87 Evron, "Authoritatively, Who Was Behind the Estonian Attacks?"; Grant, "Victory in Cyberspace," 6; and Ashmore, "Impact of Alleged Russian Cyber Attacks," 25.

term planning;[88] that Russia possesses an asymmetric strategy that it employs against its increasingly West-leaning neighbors;[89] that Soviet and Lenin tactics were applied;[90] and that Russian law enforcement agencies refused to cooperate with their Estonian counterparts in identifying the people behind the attacks.[91]

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 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 during and after WWII and which gained their independence after 1991. Its foreign policy strategy has been aimed at containing both Western influence in its neighboring countries and the advance of NATO facilities toward the Russian border.[92]

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 with 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 safe 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

88 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 were advanced by Russian nationalist "geeks."

89 Blank, "Web War I," 230.

90 *Ibid.*, 230.

91 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. According to an interviewee, Estonian authorities preferred this affair to remain low-key. Interviews with the author.

92 Mützenich, "Die Nutzung Neuer Medien Als Instrument."

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."

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 departments bore the costs of delegating their staff to handle incident response 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 neighboring 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 illegitimate 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 endeavor 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 policymakers 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 democratic 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. Today, the location of briefings for high-

level politicians by the security community now routinely takes place at Estonian CERTs headquarters.

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 thoughtful 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."[93] 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 technical advisory body to Estonia's National Security Council; and the CERT's hosting organization, RIA, has been granted special executive rights for future national security situations.

In an ideal world, such institutionalization 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 organization, 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.

93 Quotes from interviews with the author.

The Russo-Georgian War 2008

Andreas Hagen[1]

The cyber attacks against Estonia in 2007 demonstrated the degree to which nations might persuade patriotic hackers and cyber professionals to exert pressure on a hostile nation. These techniques had yet to be matched with military might. This changed in August 2008 during the South Ossetia War, when traditional Russian forces invaded the Republic of Georgia with the concurrent support of Russian hackers. The conflict between Russia and Georgia centered on a territorial dispute over the independent regions of Abkhasia and South Ossetia in Georgia, which have local independence movements supported by Russia. In 2008, Georgia attempted to reassert its control over South Ossetia, and Russia responded with significant force, invading Georgian territory in conjunction with a strong cyber offensive. Cyber capabilities had been used in conflicts before 2007; however, these actions represent singular operations rather than a campaign of cyber attacks, making 2008 important. It is the length and scope of this cyber attack, and also its effect on the population, which sparked global fears over the potential of future cyber wars.

History and Reasons for War

Russia and Georgia share a long history of differences that reach back to the annexation of Georgia to Russia in the nineteenth century and to the beginning of the Soviet Union in the early twentieth century. These differences have been brewing ever since and have resulted in violent ethnic clashes. After the Soviet Union collapsed in the early 1990s, multiple leaders of ethnic regions in the successor states demanded instant autonomy from the new governments in the former satellite states.[2] Early demands by ethnic regions like South Ossetia and Abkhazia were seen as reasonable at first. But the demands for autonomy soon escalated and turned confrontational, once they were pushing the limits the governments were willing to make. The resulting violent ethnic separatism between Georgia and the regions of Abkhazia and South Ossetia was constantly influenced by Russia.[3] Before 2008, Russia had tried to influence the Georgian economy by blocking trade and by other means of economic pressure.[4] Russia stood on the side of the minorities and supported them, mostly due to a 1992 law that allowed former Soviet Union citizens to apply for Russian citizenship. Many of the people in the neighboring regions had

1 Andreas Hagen is an analyst specialized in International Relations and Security Studies with a regional focus on Africa and Asia-Pacific. He holds a Masters degree from the Institute of World Politics in Washington, D.C. and received his Bachelor of Arts with honors in International Relations and Diplomacy from Schiller International University. He has been awarded the second place in the AFCEA/CCSA Cyber History Contest for this case study on the cyber attacks in Georgia in 2012.
2 George, The Politics of Ethnic Separatism in Russia and Georgia, 13.
3 Smith, Interview by Andreas Hagen, 17 September 2012.
4 *Ibid.*

taken advantage of this law.[5] This made Russia a key player in any discourse between the parties, as the nation often invoked the right to intervene for its citizens. To further ensure their constant involvement in any negotiations, Russia aided the regions financially. They also left small military peacekeeping forces in both Abkhazia and South Ossetia after violence broke out in those places in the early 1990s, causing tensions to run high.[6] These disagreements resulted in minor aggressions and occasional posturing.

Saakashvili began to rapidly build up Georgian military capabilities. This build-up only increased the distrust among the regional factions. Georgia implemented several anti-corruption reforms targeted at stopping smuggled imports from Russia, which represent a substantial portion of the economy of South Ossetia.[7] These reforms, combined with heightened rhetoric by senior Georgian officials, caused tense relations that were only worsened by the Russian interest to block Georgian aspirations for NATO membership.[8]

As relations between the parties deteriorated, both Russia and Georgia seem to have taken preemptive measures to ensure their security. Signs of a pending conflict led Russia to hold military exercises (called "Kavkaz-2008") at several points of the border with Georgia.[9] From mid-July to August 2008, Russia had 8,000 soldiers and heavy military hardware in the area, remaining on high alert even after the exercises had ended.[10] One of these exercises involved a hypothetical attack on Abkhazia and South Ossetia (apparently designed as an attack by a country symbolizing Georgia), against which Russian forces practiced a counter-attack to protect their interests (i.e., Russian citizens).[11] In this military exercise, Russian troops received a leaflet indicating exact Georgian troop compositions, strengths and weaknesses, as well as a reminder to be prepared.[12]

These actions suggest that Moscow was intentionally showing force to maintain their traditional regional dominance. In the months leading up to the Georgian incursion, Georgia experienced violent exchanges with South Ossetian militias.[13] While Georgia had hosted a military exercise with troops from the United States and other regional neighbors to increase interoperability between NATO and coalitions forces in Iraq, most of these troops had already left before the fighting with the Russians began.[14]

Finally, in the evening of 7 August 2008, the Georgian military entered the South Ossetian

5 Weir, "Russia-Georgia conflict: Why both sides have valid points."
6 *Ibid.*
7 George, The Politics of Ethnic Separatism in Russia and Georgia, 183.
8 Weitz, Global Security Watch: Russia, 133.
9 Berryman, "Russia, NATO Enlargement, and 'Regions of Privileged Interests,'" 234.
10 *Ibid.*, 234.
11 Nichol, "Russia-Georgia Conflict in August 2008," 4.
12 Cornell and Starr, The Guns of August 2008: Russia's War in Georgia, xi - xii.
13 George, The Politics of Ethnic Separatism in Russia and Georgia, 181.
14 Nichol, "Russia-Georgia Conflict in August 2008," 4.

capital and several other villages, claiming that they were responding to bombardments by South Ossetian soldiers that were in violation of a previously established cease-fire.[15] On 8 August 2008, Russia responded to the Georgian invasion of South Ossetia with superior military force, because they saw the Georgian actions as a threat. This was the first time that Moscow deployed its military forces outside of its borders since the war in Afghanistan ended in 1989.[16] Though both Russia and Georgia disputed the other side's justifications for intervention, they both entered into this war, which ultimately ended in a show of Russian superiority and the degradation of the long-term effectiveness of the Georgian military.[17]

Cyber Attacks: Their Importance and the Techniques

Prior to and throughout the conflict, Georgia was targeted by intensive and increasing cyber attacks against governmental and civilian online infrastructure. The cyber component in the 2008 South Ossetia War focused largely on the denial and degradation of Georgian communication systems.[18] The most important result was the essential freeze imposed upon the Georgian government's ability to use the Internet to issue any communications to their population or the outside world. Internationally, this meant the Russian version of events tended to predominate.[19] While technically less sophisticated, hackers also infiltrated numerous Georgian websites and defaced them for Russian propaganda purposes.[20]

These attacks were not only designed to control the flow of information or influence people's perceptions. They were also part of information exfiltration activities that were designed to steal and accumulate military and political intelligence from Georgian networks.[21] These activities occurred in waves and featured different techniques that ranged from distributed denial of service (DDoS) attacks to website defacements.[22] Though these attacks utilized simple methods, they were executed in more robust and interesting ways than the similar techniques used against Estonia.

Georgia had a relatively low number of Internet users and a low overall dependence on IT-based infrastructure. However, their access and dependence had been steadily increasing over the years leading up to the conflict.[23]

The coordination for the cyber attacks appeared to have been implemented weeks before

15 George, The Politics of Ethnic Separatism in Russia and Georgia, 182.
16 Ziegler, "Russia, Central Asia, and the Caucasus after the Georgia Conflict," 155.
17 Weitz, Global Security Watch: Russia, 150.
18 Hollis, "Cyberwar Case Study: Georgia 2008," 3.
19 Wentworth, "You've Got Malice."
20 Hollis, "Cyberwar Case Study: Georgia 2008," 3.
21 Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government."
22 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 4.
23 Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 5.

any shots were fired between the adversarial parties. Reports suggest that there had been streams of data directed against Georgian government sites and their Internet assets as early as 19 July 2008.[24] Hackers used DDoS attacks against the website of the President of Georgia, Mikheil Saakashvili, and were able to overload the site with requests which made it unavailable. This forced operators to take the site down for twenty-four hours.[25]

This first attack in itself did not raise great suspicion among the international community, mostly because the Georgian President downplayed the significance of the single attack.[26] Only cyber security experts suspected that some of the toolkits used in the attack originated from the Russian regional sphere. This was due to the language used in the code, as well as the obvious statement "win+love+in+Rusia" embedded in some of the messaging.[27] After the initial cyber attack at the end of July, there had not been much activity before the conflict, aside from what in hindsight appears to have been preparations or reconnaissance for the major attacks in August 2008.[28]

Concurrently with the Russian invasion of Georgia, cyber attacks started to increase in number and in sophistication. In addition to the Georgian President's website, cyber attacks targeted the pages of the Parliament, the Foreign Ministry, the Interior Ministry, several news agencies, and a few banks.[29] This disruption of methods of communication denied the Georgian government the ability to effectively communicate with its citizens via the Internet or to deliver their own version of events to the world. Also among the first targeted websites were Georgian hacker forums.[30] These attacks were not entirely successful, but appear to have been designed as a preemptive strike against any possible retaliatory attacks from Georgian hackers.

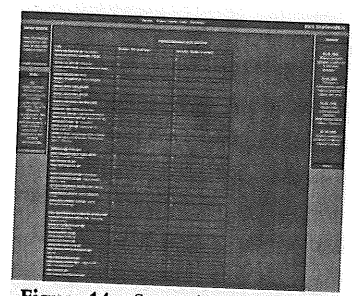

Figure 14: Screenshot of a list of 'potential' targets on StopGeorgia.ru

The hackers utilized sophisticated DDoS methods against targets, incorporating SQL injections and cross-site scripting (XSS).[31] These methods allow fewer users or smaller botnets to achieve the same results.[32] Besides the distribution of the DDoS tools through various websites, "StopGeorgia.ru" also contained a list of potential target sites to attack,

24 Markoff, "Before the Gunfire, Cyberattacks."
25 Danchev, "Georgia President's web site under DDoS attack from Russian hackers."
26 Nazario, Interview by Andreas Hagen, 30 October 2012.
27 Nazario, "Georgia on My Mind – Political DDoS"; and Nazario, Interview by Andreas Hagen, 30 October 2012.
28 Markoff, "Before the Gunfire, Cyberattacks."
29 Wentworth, "You've Got Malice."
30 Keizer, "Russian Hacker 'Militia' Mobilizes to Attack Georgia."
31 Carr, Inside Cyber Warfare, 3.
32 Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks."

including sites from governmental institutions (Figure 14).[33] These methods indicate that some basic-level planning and coordination had occurred within Russia's hacker forums.[34]

In addition to DoS attacks, several Georgian websites experienced defacements as well. The online hackers utilized several picture collages that depicted and compared the Georgian President Mikheil Saakashvili with postures of Adolf Hitler (See Figure 15).[35] Defacements of this type and other pro-Russian propaganda were found on the websites of the Georgian President, the National Bank of Georgia, and the Ministry of Foreign Affairs, which later were targeted by DoS attacks.[36]

The cyber aggressors also attempted to sway initial international public opinion concerning the conflict by trying to manipulate non-scientific quick-votes online, on sites like CNN, while blocking access to major international media sites inside Georgia.[37] This helped the Russian bloggers to influence initial perceptions and make Russia's actions appear to be justified as a peacekeeping intervention. Such efforts, in connection with the unreliable communications during the conflict, were no doubt intended to generate initial support for the Russians, at least until the deception was discovered. Such rather minor actions, though not considerably harmful, created nuisances that diverted focus and necessary attention.

The cyber attacks on the banking sector in Georgia had several repercussions that affected everyday life in Georgia and made the period of the invasion more difficult for the population.[38] The persistent attacks on the systems of several banks forced them to shut down their electronic services until the threat had passed.[39] This not only significantly disrupted the connection to foreign banks, but also apparently paralyzed the Georgian payment system, leaving some Georgians without access to money. Due to limited or zero access to financial means, many Georgians could not buy anything in stores. This in turn significantly decreased demand for goods during that time.[40]

Figure 15: Images used comparing Saakashvili to Hitler

33 Danchev, "Coordinated Russia vs Georgia cyber attack Cyber Attack in progress."
34 Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks."
35 Danchev, "Coordinated Russia vs Georgia cyber attack Cyber Attack in progress."
36 Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 7.
37 Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia."
38 Schönbohm, Germany's Security - Cyber Crime and Cyber War, 49.
39 Rhodes, Cyber Meltdown, 36.
40 Smith, Interview by Andreas Hagen, 17 September 2012.

Georgian Cyber Defenses

The Georgian government's cyber defense capabilities were very limited and spread thinly, due to the scale of the conflict on the ground as well as the barrage of cyber activities on their systems. The Georgian's first response to the massive amounts of activity in their Internet infrastructure was to establish filtering mechanisms that would lock out any Russian IP-address from accessing Georgian networks.[41] The bulk of attacks originated from servers located in Russia. This method was rather ineffective, because the hackers expected such behavior and adapted quickly by circumventing these filters through accessing the Georgian systems over servers in other countries apart from Russia. The Georgian government also immediately contacted Estonian officials in the hope of gaining access to their vast expertise after the 2007 cyber attacks in Estonia, and also because there was no other international organization they could address for help.[42] The Estonians provided informal access to some of their own cyber security experts and also sent two of their information security experts to Georgia in order to assist locally with the defense.[43] But even with their cooperation, they were unable to mitigate any of the attacks effectively. Thus, these Estonian experts mostly worked on damage control.

Georgia does not have an Internet exchange point (IXP), and they are therefore very dependent on neighboring countries like Turkey, Armenia, and Russia (almost 70 percent).[44] The only really effective defensive countermeasure the Georgians used in order to keep some of their information channels to the public open was the transfer of cyber assets and websites to servers in countries like the United States, Estonia, and Poland.[45] These measures were often undertaken by third parties, such as private businesses, rather than official host countries like the US government.

The Georgian President's website was transferred to Google blog servers in California, the Ministry of Defense website to a private business in Atlanta, the Ministry of Foreign Affairs site to servers in Estonia, and the Office of the President of Poland allowed its website to disseminate information on behalf of the Georgian government.[46] The owner of Tulip Systems in Atlanta offered his services to the Georgian government in order to protect Georgian Internet interests, but without any official approval by the US government.[47] After the conclusion of the conflict, the company reported that it experienced cyber attacks against the website that was taking refuge on their servers.[48] This relocation of cyber

41 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 7.
42 *Ibid.*
43 Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 15.
44 *Ibid.*, 6.
45 *Ibid.*, 14.
46 Clarke and Knake, Cyber War: The Next Threat to National Security and What To Do About It, 19; and Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 14.
47 Korns and Kastenberg, "Georgia's Cyber Left Hook," 66-67.
48 *Ibid.*, 67.

assets could have involved the United States, Poland, or Estonia in the Russo-Georgian conflict politically or militarily.

However, during the attacks on the Georgian Internet infrastructure, the Georgians were not only on the defensive. Once the ramifications and the impact on the Georgian cyber infrastructure were realized, more international support from unlikely places poured in as well. A few German hackers tried to redirect Georgian Internet traffic through a German server to keep the websites up and running. They managed this only for a few hours in the initial stages of the conflict, until their efforts were intercepted and rerouted through servers in Moscow.[49] After the initial attacks and their failure to completely take down local hacker forums, Georgian hackers began to mobilize as well. They retaliated with their own denial of service attacks. The Georgians targeted the website of a Russian news service based in Moscow, called RIA Novosti.[50] According to the US Cyber Consequences Unit report, another counter-attack effort by the Georgians was the distribution of an attack tool designed to be used by Russian sympathizers who would unknowingly attack Russian websites instead of Georgian sites.[51] Retaliations of this kind were very limited and rather ineffective, due to the massive influx of attacks from Russian sources and the apparent "preparedness" of the Russian hackers.

Origin of the Cyber Attacks and Their Possible Connections[52]

Overall, these cyber attacks on Georgian systems and networks spanned over several weeks, from before the conflict had started to after it had ended. However, the main bulk of the attacks coincided–and perhaps were also coordinated–with Russian forces attacking on the ground during the five day Russian incursion that started 8 August and lasted until the ceasefire agreement on 12 August 2008.

After the conflict, there were many accusations, which identified several different groups as perpetrators of the attacks. These groups included the Russian military, their secret intelligence services (i.e., the FSB), Russian nationalists, and even Russian organized crime syndicates. It is likely that all of these groups could have had some (if only limited or indirect) involvement with the cyber attacks.

Despite technical difficulties in attribution, several cyber security analysts concluded that the bulk of the attacks originated from servers that were located in the Russian Federation.[53] There were also signs that an increasing number of pro-Russian sympathizers

49 Espiner, "Georgia accuses Russia of coordinated cyberattack."
50 Keizer, "Russian Hacker 'Militia' Mobilizes to Attack Georgia."
51 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 7.
52 See the Concluding Assessment of this book for additional analysis of the national responsibility for the Georgian attacks.
53 Espiner, "Georgia accuses Russia of Coordinated Cyberattack"; and Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 2.

from other countries, such as the Ukraine and Latvia, soon began participating in some form as well.[54]

In addition, over the past several years, there has been major mobilization in a hacker underground movement located in Russia. Participants often speak out on political issues, and virtually or literally invite involvement by way of nationalistic articles in the Russian media.[55]

Just before the increased volume of the cyber activities were registered, several Russian web forums and hacker sites became active against Georgia. Sites like "xaker.ru" (in English: hacker.ru), "stopgeorgia.ru," and "stopgeorgia.info" began rallying for the Russian cause and encouraged would-be cyber militia members through the use of propaganda. They also distributed of a static list of targets and provided cyber tools with instructions.[56] Security analysts found that many of these sites catered to a specific demographic and nationality, because access from US-based addresses and computers was quickly banned or restricted.[57] At these sites, there was a large cadre of knowledgeable hackers, who assisted beginners with their hacking techniques.

This top-down hierarchy was also the supplier of the instructions and tools that allowed beginners to evade security firewalls and disguise their tracks to circumvent any Georgian countermeasures.[58] Such specialized knowledge and sophistication again suggests some sort of support from the Russian government or military. Some elements could have easily been inside that hierarchy. A Russian defector admitted once that Russian hackers convicted of cyber crimes were often given a choice to work for the intelligence services instead of going to prison.[59] Such hackers, under the control of the government, could easily direct and give instructions to beginners while completely disguised under a random username in a forum.

> *When one considers the forensic evidence, geopolitical situation, timing, and the relationship between the government, the youth, and criminal groups, it is not difficult to conclude that the Kremlin was behind it all.*
>
> David J. Smith, Russian Cyber Operations, Potomac Institute Cyber Center

Once the targets, tools, and instructions were provided and online for everybody to obtain, the Russian cyber militia began to mobilize themselves like a chain reaction. Many of the hackers began collaborating over well-known social media portals like Twitter and

54 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 3.
55 Danchev, "Georgia President's web site under DDoS attack from Russian hackers."
56 Danchev, "Coordinated Russia vs. Georgia cyber attack in progress."
57 Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks."
58 *Ibid.*
59 *Ibid.*

Facebook.[60]

Such a cyber militia, comprised of enthusiastic nationalists and hackers, can be very devastating but also very beneficial for a government. Because there is no "visible" connection between the government and the "voluntary" hackers, deniability is much easier. On the other hand, the actions of the militia cannot be directly controlled unless they are preplanned. Indications for such organization can be found in the specific distribution of targets, tools, and instructions. Therefore, it is still unclear if the cyber militia acted alone or was instigated by the Russian government itself.

Accumulating evidence points to a St. Petersburg-based criminal cyber gang known as the Russian Business Network or RBN.[61] Many of the attackers against Georgia apparently used tools, attack commands, and servers that have been attributed to this Russian organized crime outfit. The RBN has been known to contract its services to third parties, and since there has not been any major attempt by the Russian government to shut down this organization, that absence of action could suggest it is being endured, if not employed, for its services.[62]

Other Russian organized crime groups were involved, such as Stopgeorgia.ru, which has been involved in creating fraudulent passports and credit card scams. The Russian authorities were rather inactive in investigating these activities.[63] A few reports also suggest that the Russian "patriotic hackers" might have been actively hired to perform cyber attacks or reconnaissance under the mantel of a group called Nashi, which has been known to enforce the will of the Kremlin in internal and external matters.[64]

So the role of Russian hackers and organized crime groups seems established. What about the Russian government?

Russia is characterized by a unique nexus of government, business, and crime.

David J. Smith

Ever since the fall of the Soviet Union and the restructuring of the main intelligence service, the KGB, there have been allegations that there are likely ties between the Russian government, organized crime syndicates, and business corporations around Russia. Connections between government, business, and crime are a unique part of Russian society and culture.[65] In Russian society, there occasionally seems to be no clear distinction

60 Gorman, "Hackers Stole IDs for Attacks."
61 Markoff, "Before the Gunfire, Cyberattacks."
62 Wentworth, "You've Got Malice."
63 Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," 13.
64 Carr, Inside Cyber Warfare: Mapping the Cyber Underworld, 115-117.
65 Smith, Interview by Andreas Hagen, 17 September 2012.

between the government and the criminal underworld, and criminals often share significant contacts with business oligarchs, politicians, and vice versa.[66] Other allegations suggest that the Russian government or parts of the ultra-nationalist Liberal Democratic Party of Russia (LDPR) employ criminal organizations or mafias as an extension of political power, utilizing them in cases in which the government cannot "officially" act.[67]

The involvement of the suspicious Russian Business Network also suggests that this wave of cyber attacks against Georgia was not an unplanned and spontaneous occurrence. There is a strong sense of coordination behind the operation, because they tried to conceal the true origin of the attacks. The Open Source Intelligence report *Project Grey Goose* presented an analysis of the cyber attacks in Georgia; this discusses a piece of Russia's cyber strategy described in a Russian military journal, which emphasizes the need to disguise information warfare or cyber attacks as criminal activities in order to obtain deniability:

> *The practical part of the problem is that the target of a cyberattack, while in the process of repelling it, will not be informed about the motives guiding its source, and, accordingly, will be unable to qualify what is going on as a criminal, terrorist, or military-political act. The more so that sources of cyberattacks can be easily given a legend as criminal or terrorist actions.*[68]

Though there are still a few pieces missing that would establish a concrete connection with the Russian government and military, the coincidence of a coordinated attack from the Russian ground forces and the invisible cyber forces still seems far from random. Both the Russian Business Network (RBN) and Nashi, a Kremlin supported youth group, are known to have cyber capabilities and could have served in an organizing role during the conflict. Either organization might have had a communication link with the Russian military, or even a concrete command and control hierarchy. This seems all the more likely, considering the simultaneous mobilization of Russian forces on the border with Georgia, the reconnaissance work in Georgian networks by hackers, and the first wave of cyber attacks coinciding almost exactly with the first Russian aerial bombing runs.[69]

Outcome and Lessons for the Future

Besides the economic benefits for Russia that resulted from the conflict, the use of the "unofficial" Russian cyber militias has proven to the world the effect that such an instrument can have on a conflict. Not only did these rather crude cyber efforts disrupt vital lines of communications to the people in the crisis, as well as to the international community; they also had a psychological effect that intensified the fears of the public.

66 Burton and Burges, Russian Organized Crime.
67 Harding, "WikiLeaks cables: Russian government 'using mafia dirty work.'"
68 Moscow Military Thought (English), Russian Federation Military Policy in the Area of International Information Security, quoted in Greylogic, "Project Grey Goose Phase II Report: The evolving state of cyber warfare."
69 Goodin, "Georgian Cyber Attacks Launched by Russian Crime Gangs."

If such cyber measures increase in sophistication in the future and are applied to a fully developed communications network, then they may have an even more amplified effect compared to the situation in Georgia. The international community, especially the United States, often underestimate the value of such cyber militia groups, whereas countries like Russia, Iran, and China have been encouraging them for a long time, which places the United States at a strategic disadvantage.

These cyber attacks on Georgia have proven to Russia once again that the use of a cyber militia or "independent" hackers like the RBN or Nashi could impact a nation's economy or public perceptions without causing a severe international response.[70] The use of cyber militias has gradually increased over time, giving countries like Russia, China, and Iran, all of whom engage in this tactic, the opportunity to strengthen their cyber warfare capabilities, as seen in the Russian campaigns against Estonia (2007), Lithuania, (2008), and Kyrgyzstan (2009). The Russian government has been benefiting from these situations while always keeping their deniability intact. The use of cyber militias might become a norm for Russian political interaction in the future, since it has been proven useful both in peacetime and in tandem with military operations.

The Russian cyber militia seems to represent a variable which has not been fully explored in the planning of war scenarios by many intelligence and military services. Because of the Russian government's deniability concerning the activities of their civilian cyber force, the militia could be utilized for an array of intelligence functions. Not only can they be called upon in conflict situations; they also could prove useful in intelligence gathering or in denial and deception operations, because their activities in peacetime are still seen as mediocre crimes instead of threats to national security.

70 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 8.

Part 6: Concluding Assessment

"Pointing the Finger" – National Responsibility For Cyber Conflicts

Jason Healey

What nations are behind these cyber conflicts? It may be too early to apply the judgment of history, but not so early for the judgment of this particular historian.

This chapter applies the ten-point "spectrum of state responsibility" from the Atlantic Council (see Table 3 on page 50) to help determine which nation bears the national responsibility for initiating three of the cyber conflicts in this book: Estonia, Georgia, and Stuxnet. [1]

Attribution of cyber attacks has been the most difficult, yet the most important, aspect of cyber defense. However, remember one of the key lessons of history: the more strategically significant the conflict, the more similar it is to conflicts in the other domains. Attribution, which usually starts at the most technical level before working up to the people and organizations responsible, usually is not a helpful approach for such strategically important cyber conflicts.[2] There will always be analysts who say, "you cannot prove that" or "the source of the attacks might be faked." These small technical truths have for too long obscured the larger truths of which nation was responsible.

So rather than this bottom-up, technical analysis, this chapter will employ a non-technical, top-down analysis, far more likely to aid decision-makers. The key question they need to answer is not "who did this?" but "what nation, if any, is responsible?"

Attack more likely to be non-state-sponsored if:

- Not traced to nation
- Not traced to state organizations
- Attacks not written or coordinated in national language
- Low state control over the Internet
- Low technical sophistication
- Low targeting sophistication
- Broad popular anger at target
- Direct commercial benefit
- No state support of hackers
- Public statements from hackers
- Openness and cooperation with the investigation
- Little correlation with national policy
- Many other nations or groups that benefit
- Not correlated or integrated with physical force

1 See Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks."

2 A typical attribution chain of analysis will typically go something like this: find the computers most directly involved -> find the computers controlling those computers, the command and control (C2) -> find the identity controlling the C2 computers -> determine which person is associated with that identity -> find links between that person and an organization -> look for evidence that the organization is under formal state control. Each next step in the chain becomes progressively more difficult.

Analyzing National Responsibility

This spectrum shows a full range of how nations can be responsible for attacks by ignoring, abetting, or conducting cyber attacks. At levels one and two, the nation will stop the attack if they can. At levels three and four, the nation is ignoring or encouraging the attack but not truly "sponsoring" it. At levels five and six, the nation is clearly the sponsor, as the group is getting very active support. Above that, from levels seven to ten, the nation itself is in *de facto* control over the attack. Any non-states involved are direct proxies, under the control of the state, and the attacks are state-sponsored.

Too often, technical tools and methodologies are unable to determine where an attack lies on the spectrum.[3] Fortunately, there's a rich tradition of analysis in the technical disciplines—as well as in the intelligence, law enforcement, and legal professions—which can guide us.

Fourteen key elements (see the text boxes on this page and the next) appear to have been central in analyzing attribution for attacks and attack campaigns over the past decade. Many are particularly helpful to analyze attacks that purport to be from "patriot hackers."

Few of these elements have strong attribution power on their own, or can be relied upon to attribute an attack with little or no other evidence relating to other identifying categories. But taken together, they can provide a compelling case. Analysts can make better, more confident assessments when we have strong evidence, corroborated from multiple sources, across many independent categories.

The strongest elements are attacks technically traced to state organizations, statements from national leadership ("Yes, we did it."), direct support of hackers, and attacks correlated or integrated with physical force. The weakest elements are attacks traced to the nation as a location of origin and assessments of the nation's technical sophistication.

Attack more likely to be state-sponsored if:

- Traced to nation
- Traced to state organizations
- Attacks written or coordinated in national language
- State control over the Internet
- Technical sophistication
- Targeting sophistication
- Little popular anger at target
- No direct commercial benefit
- Direct state support of hackers
- Strong correlation with statements from national leadership
- Lack of openness and cooperation
- Strong correlation with national policy
- Lack of any other nation or group that benefits
- Correlated or integrated with physical force

3 Verizon has found that of two-thirds of the incidents they investigated in 2009 were untraceable to a specific identity, other than an IP address, even when they were working with law enforcement. See the excellent Verizon Data Breach Report for 2008 (p.18) for this percentage and other hard data, which were incorporated in their updated 2009 report. Amazingly, the highly sophisticated attacks led to 95 percent of the total compromised data records. The 2008 report can be found at: http://www.verizonbusiness.com/resources/security/databreachreport.pdf. The 2009 report is here: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

Unfortunately, a common analytical mistake in the past has been to "connect the dots" for an attribution—meaning to develop a plausible attribution based on only one or a few (and usually the weakest) elements. These "just-so stories" could be one possible attribution, but often do not look across all the elements, and/or they ignore exculpatory evidence. This can lead to mistaken attribution and lack of credibility for the decision-makers.

Attacks are more likely to be proven state-sponsored if analysts can develop solid evidence across each the following elements:

- **Attack traced to a nation.** Though attacks routinely are routed through or originate from third countries, many large-scale attacks do indeed seem to be tied to their apparent national origin. The attack source information can be faked, but patriotic hackers often do not bother. Still, this element is only a weak link to state sponsorship.
  - Examples: the Hainan Island Incident, 2001;[4] Estonia, 2007;[5] Georgia, 2008.[6] Many attacks against the US, Estonia, and Georgia were traced to China and Russia, which corroborated other analytical elements to help attribute the attack.
- **Attack traced to state organizations.** Only rarely do analysts find this kind of evidence, but it provides a very strong link—especially if the state organization has a law enforcement or security role.
  - Examples: Falun Gong, 1999. After a crackdown in China, a Falun Gong website in Canada was attacked by a denial-of-service, which persisted even when the site was mirrored in the US. Some (but not all) of the attacks traced directly to China's Ministry of Public Security, which was, as now, under pressure to crack down on the group.[7]
- **Attacks written or coordinated in national language.** Though they may be written to misdirect and confound defenders, malicious codes usually at some level contain language clues or other cultural artifacts. Similarly, coordination of larger, denial-of-service attacks often takes place over the Internet and in a particular language which can be applied to attribution.

4 The US was attacked with a wave of defacement attacks after a Chinese interceptor collided with a US EP-3 reconnaissance aircraft, which subsequently crash-landed on Hainan Island, China.

5 Eniken, Kaska, and Vihul. "International Cyber Incidents: Legal Considerations," 23. Ethnic Russians protested in Estonia and conducted cyber attacks due to the removal of a statue of a WWII Russian soldier.

6 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 2. Russian military forces invaded Georgia, and the physical invasion was accompanied by cyberattacks, after months of international tension.

7 Details on this largely forgotten state-sponsored attack can be found in Chase and Mulvenon, You've Got Dissent, 71-76.

- Examples: GhostNet, 2009; Georgia, 2008. The GhostNet intruders used a Chinese-coded remote access control tool.[8] The discussions coordinating the Georgian attacks of 2008 took place over social networking sites, and all but one were in the Russian language.[9]

- **State control over the Internet**. Attacks coming from a country which keeps tight reins over the Internet are slightly more likely to be state-sponsored, since those governments have more options to control information traversing their networks.

  - Examples: the Hainan Island incident, 2001. China has always tried to maintain tight limits on the use of the Internet by its citizens; that control is also believed to exist in Russia and other nations of the Shanghai Cooperation Organization. So, the defacement and denial-of-service attacks coming from China in 2001 were more likely to be state-sponsored than similar attacks from more liberal nations.

- **More technical sophistication than normal**. This analytical element too often misleads, as most analysts mistakenly assume that only nations have the ability to create sophisticated attack tools. Moreover, the reverse is also true: nations may use an unsophisticated tool, if it will still do the job. Indeed, some analysts felt BUCKSHOT YANKEE could not be state-sponsored because Agent.btz was so simple.

  The most incriminating technical sophistication is often not the technical tool itself, but any use of insiders, supply chain intervention, and other patient and resource-intensive methods of access. Therefore, be exceptionally cautious and skeptical when attributing using this analytical element.

  - Examples: Stuxnet. This malware was so sophisticated that it is far more likely to be from a nation. It exploited multiple high-value, previously unknown vulnerabilities, was designed to be under tight control, and targeted a very rare industrial control system, requiring extensive testing on similar equipment.[10] Such an operation is beyond all but the most committed non-state groups.

- **More targeting sophistication than normal**. Attacks are less likely to be state-sponsored if they are against public webpages of organizations unrelated to a current conflict or without strategic purpose. State-sponsored attacks are more likely to be narrowly aimed toward targets supporting the military or government, critical infrastructure control systems, and related targets. Supporting evidence can come from knowing the extent of targeted organizations or discovering attack vectors crafted to attack only specific targets of choice.

  - Examples: GhostNet, 2009; Stuxnet. The GhostNet intruders used attack tools which were narrowly and individually crafted against the organization supporting the Dalai Lama.[11] This implicates the Chinese government, which accuses him of feeding separatism in Tibet.[12] Stuxnet was even more narrowly targeted to only disrupt a system configuration that existed in one place in the world, Iranian nuclear facilities.

- **There is only narrow government anger** (rather than broad societal fury) at the target. This category is helpful to distinguish state attacks posing as patriotic hacking.

  - Examples: Chinese Embassy Bombed in Belgrade, 1999; China's anger at Falun Gong, 2000; the Hainan Island incident, 2001; GhostNet, 2009. These examples highlight how the depth of public anger can help to determine national responsibility. Both after NATO bombs accidentally destroyed the Beijing embassy in Belgrade[13] and the Hainan Island incident, Chinese cities were rocked with angry demonstrations, fed by genuine public anger. The resulting defacements and denial-of-service attacks were easily attributed to patriotic hackers[14] (though perhaps encouraged or assisted by Chinese leadership).

    On the other hand, the similar attacks against the Falun Gong[15] are not so easily attributed to patriotic hackers, as the populace does not seem to share the Chinese leadership's prominent concern about this religious group. Some Chinese citizens do feel strongly about Tibet and Taiwan being integral parts of China, so GhostNet fits neatly between the first two examples.

- **No direct commercial benefit**. Verizon has found that 55 percent of the incidents they investigated over four years affected the retail or food and beverage sectors[16] with payment records (e.g., credit card data) accounting for 84 percent of the total records compromised.[17] Groups driven by criminal motives are far more likely than most nations to target this kind of data, so these are less likely to be state-sponsored. Incidents targeting military research and development, political decision making, and other less commercial interests are more likely to have a state-sponsored link.

8 Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," 46. The report reveals an extensive cyber espionage network with many links to China.
9 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 3.
10 See the chapter by Chris Morton on Stuxnet in this book.
11 Information Warfare Monitor, "Investigating GhostNet," 20.
12 Information Warfare Monitor, "Investigating GhostNet," 42-43.
13 See the BBC summary "1999: Chinese Anger at Embassy Bombing."
14 The National Infrastructure Protection Center (housed at the Federal Bureau of Investigation) warned US companies to prepare for a wave of Chinese patriotic hacking. For a summary of the events, see Hulme, "NIPC Warns of Chinese Hacktivism."
15 Several cases from 1999 onward are discussed in Chase and Mulvenon, You've Got Dissent, 1-44.
16 Verizon Business Risk Team. "Verizon Data Breach Report 2008," 8.
17 Verizon Business Risk Team. "Verizon Data Breach Report 2008," 21.

- Examples: GhostNet, 2009; Koobface, 2010. The GhostNet attackers compromised NATO SHAPE headquarters, embassies, foreign ministries, and the office of the Dalai Lama.[18] As none of these were likely to lead to direct financial gain, it helps add weight to a state-sponsored attribution. By contrast, the gang behind Koobface were only interested in money, which they collected on a grand scale through fraud, though pennies at a time. Such crime might be ignored or encouraged by governments, but it is less likely to be the government itself.[19]

- **Direct support of hackers**. Evidence of direct government support of attacking groups would be particularly damning evidence, though it is rare to find. Governments usually try to keep their involvement covert; officials acting without official cover will be similarly slippery. When determining national responsibility, analysts cannot simply infer such support from related evidence. To qualify for this category, evidence should be suitably straightforward. Circumstantial evidence is not enough.

  - Examples: Georgia, 2008. Some analysts who investigated the attacks on Georgia assessed that the cyber attackers had been tipped off about impending Russian military operations: "the signal [to attack specific targets] had to have been sent before the news media and general public were aware of what was happening militarily."[20]

- **Attack correlated with public statements**. Public statements are the most easily collected pieces of evidence, as they are found online or in that nation's media. Hackers will often boast of their participation in defacement or denial-of-service attacks, while national leadership can make public statements encouraging or discouraging attacks. When they seem to encourage attacks, these statements make the nation more responsible for the resulting attacks (even if they are actually undertaken by patriotic hackers). Conversely, statements from leadership calling for restraint and promising prosecution of hackers make it less likely.

  - Examples: Chinese Embassy Bombed in Belgrade, 1999; Estonia, 2007; US Patriot Hacking, 2003. After the NATO bombing of the Chinese Embassy in Belgrade, the Chinese national leadership was enraged at the US, and their comments helped fuel the physical and cyber attacks against the US. Chinese hacker groups like l10n and HUC operated openly, with seemingly little fear of punishment from China.[21] Only after the protests had lasted for several days did the Chinese leadership start making statements to restrain the attackers.[22]

    During the Estonia attacks, the Russian government made no calls for restraint. Indeed, the Russian First Vice Prime Minister called for a boycott against Estonia, and the President criticized the Estonian decision to move the statue, appearing to give a green light for physical and cyber protests.[23]

    In comparison, before the invasion of Iraq in 2003, the US warned US hackers that hacking "is illegal and punishable as a felony ... The US government does not condone so-called 'patriot hacking' on its behalf." Any attacks against Iraq were less likely to be patriotic hackers and more likely to be US state-sponsored attacks (especially as the media has since reported the US was in fact planning state-conducted attacks).[24]

- **Lack of state cooperation during investigation.** This is a common, but subjective, element of the analysis which can be incriminating or exculpatory.

  - Examples: Estonia, 2007; Operation Physh Phry, 2009. The Russian government was implicated by their rejection of Estonian requests for assistance and information during the attack campaign against their country.[25] A more positive example is the cooperation between the US and the Egyptian governments in the 2009 arrest of a large number of hackers in both countries, a compelling indication that the attacks were not sponsored by either nation.[26]

- **Attack correlated with specific national policy**. National policy can be discerned most easily from publicly released documents, research and development priorities, industrial policy, and national security objectives. Through collection of secret intelligence, analysts may be able to add to their understanding of other nations' intelligence collection priorities and other key details. Identifying a nation's intelligence priorities can be particularly helpful when attributing penetrations which steal sensitive research and development information.

  - Example: GhostNet, 2009; Stuxnet. China has made it clear for decades that Taiwan and Tibet are "inalienable part[s] of the Chinese territory ..."[27] Given the number of Tibetan and Taiwanese targets in GhostNet,[28] this makes it slightly

18 Information Warfare Monitor, "Tracking GhostNet," 42-43.
19 Villeneuve, "Koobface: Inside a Crimeware Network."
20 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 3.
21 See the chapter by Jon Diamond on patriotic hacking in this book.
22 Rosenthal, "Crisis in the Balkans, China: More Protests in Beijing as Officials Study Bombing Errors."
23 See the chapter by Andreas Schmidt on the Estonian attacks in this book.
24 Shanker and Markoff, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk."
25 Eniken, Kaska, and Vihul, "International Cyber Incidents: Legal Considerations," 29.
26 FBI Los Angeles, "One Hundred Linked to International Computer Hacking Rin
27 This is a routine Chinese official statement. For the statement about Tibet, see "China's Top Legislature Slams EU Parliament for Tibet Resolution." For a good summary of the event, see "China, Taiwan, Tibet: Fraying at the Edges."
28 Information Warfare Monitor, "Tracking GhostNet," 42-43.

more likely that the GhostNet attacks are state-sponsored. The United States and Israel were clearly aligned strongly against the Iranian nuclear enrichment program, making them more obvious culprits once Stuxnet was discovered.

- ***Cui bono?*** (Latin for "who benefits?") Often, there are only a few nations or groups that benefit from the attack, making them the plausible candidates to be behind the attack.
  - Example: Estonia; Georgia; Stuxnet. In the Estonian and Georgian cyber conflicts, only Russia was involved in a national security crisis with those two nations. So, while some of the attacks in those conflicts traced to the United States, it is still more likely (barring other lines of evidence) that Russia was more responsible than the United States. Likewise, few nations other than the United States and Israel would benefit from destruction of Iranian nuclear enrichment gear.

- **Attack strongly correlated or even integrated with physical force.**
  - Example: Chinese Embassy Bombed in Belgrade, 1999; Georgia, 2008. As noted earlier, the denial-of-service and defacement attacks from China in 1999 corresponded with an outpouring of anger and physical violence against American embassies and consulates across China. Likewise, in Georgia the cyber attacks occurred against the backdrop of a physical invasion of that country by Russia. In both cases, most attacks were easily attributable to China and Russia, respectively, so the task for analysts was to further examine the evidence looking for explicit state support.[29]

Application: Responsibility for Estonia, Georgia, and Stuxnet

This methodology is most useful for disruptive attacks, when there is usually more public information available. It would be extremely difficult, for example, to examine responsibility for BUCKSHOT YANKEE, as there is little information, and what exists has been released or leaked from only one source, the US military itself. Fortunately, there is more than enough information for three other conflicts, Estonia, Georgia, and Stuxnet.

The following table shows an analytical assessment for each of the elements introduced above concerning the cyber attacks on Estonia in 2007.[30]

29 For a very structured analysis on Georgia by the US-CCU and Bumgarner, see Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008."

30 Please note, this analysis is this author's own, and may differ from the assessment of each of the chapter authors. While analysts may rightly argue about these individual and collective judgments, having a transparent analytical framework makes it much easier to assess how the evidence is assessed.

Table 4: Analysis of the Estonian Cyber Attacks of 2007

Analytical Element	Assessment
Attack Traced to Nation	Many traced to Russia[31]
Attack Traced to State Organizations	Some traced to Russian state institutions[32]
Attack Tools or Coordination in National Language	In Russian[33]
State Control over the Internet	Partial but growing[34]
Technically Sophisticated Attack	Not particularly sophisticated[35]
Sophisticated Targeting	Not particularly sophisticated[36]
Popular Anger	Strong[37]
Direct Commercial Benefit	Low[38]
Direct Support of Hackers	No evidence
Correlation with Public Statements	Comments by both government and individuals[39]
Lack of State Cooperation	Russia refused to cooperate[40]
Cui Bono?	High: Russia[41]
Correlation with National Policy	Strong[42]
Correlation with Physical Force	Moderate[43]

31 NATO CCDCOE Report, "International Cyber Incidents: Legal Considerations," 23

32 Ibid., 23.

33 Ibid., 15.

34 For example, see Zigfield, "Re-Imposing Totalitarian Information Control in Russia."

35 Ibid., 18-20. The attacks were mostly simple denial-of-service, defacements, and spam, though there were some more sophisticated attacks on DNS servers.

36 Ibid., 20. "Notably, traditional critical infrastructure targets, such as information systems supporting transportation and energy systems, were not targets."

37 In Estonia, there were strong pro-Russian protests, with one person killed and hundreds injured and arrested: "Tallinn Tense after Deadly Riots."

38 Though commercial targets (like banks) were taken offline for some time during the attacks, there was little chance for commercial gain. However, since the purpose of the attack was disruption, not taking data, this should not weigh heavily for our attribution.

39 A "commissar" of Nashi, a pro-Kremlin patriotic youth group, claimed credit for the attacks, in an interview with Charles Clover. Clover, "Kremlin-Backed Group Behind Estonia Cyber Blitz." During the conflict, Russian President Putin seemed to egg on attackers with comments like, "Acts of mockery of the heroes and victims of war give rise to anger and indignation." "Putin in Veiled Attack on Estonia."

40 NATO CCDDCOE Report, "International Cyber Incidents: Legal Considerations," 29.

41 There were no other nations or groups that obviously benefited from attacking Estonia or were in an existing crisis.

42 For example, the Russian Parliament threatened to impose sanctions. Sheeter, "Russia Slams Estonia Statue Move."

43 As noted above, the cyber attacks coincided with violent protests by ethnic Russians; however, there was no physical invasion or other use of overt force by Russia.

This analysis demonstrates that Russia's responsibility is somewhere in the middle of the spectrum of state responsibility. With no evidence of direction or coordination, the attacks are not obviously state-sponsored. But clearly, the Russian government is not without responsibility. Here are a few possible assignments from the spectrum of state responsibility:

3. State-ignored. The national government knows about the third-party attack but is unwilling to take any official action.

4. State-encouraged. Third parties control and conduct the attack, but the national government encourages them as a matter of policy.

5. State-shaped. Third parties control and conduct the attack, but the state provides some support.

6. State-coordinated. The government coordinates third-party attackers, such as by "suggesting" operational details.

There is no available evidence supporting any nations providing "active assistance" for the attack. However, Russia does not escape all responsibility: there were clear statements from the highest levels of the Russian government, a lack of cooperation with the investigation, a clear correlation with Russian official policy, and complete failure of the government to rein in the attacks. There is an accordingly ***high confidence*** **that the attacks on Estonia were *at least encouraged*** by the Russian government. The attacks were possibly also shaped by Russia, but other than links to the Nashi youth group, there simply is not enough solid evidence.

For the 2008 attacks against Georgia, the analysis looks similar, though more damning for Russia.

Table 5: Analysis of the Georgian Cyber Attacks of 2007

Analytical Element	Assessment
Attack Traced to Nation	Many traced to Russia (and in particular to Russian organized crime)[44]
Attack Traced to State Organizations	No strong evidence[45]
Attack Tools or Coordination in National Language	In Russian[46]
State Control over the Internet	Partial but growing[47]
Technically Sophisticated Attack	Yes[48]
Sophisticated Targeting	No[49]
Popular Anger	Broad anger within Russia
Direct Commercial Benefit	Low (but inconclusive)[50]
Direct Support of Hackers	None[51]
Correlation with Public Statements	Strong[52]
Lack of State Cooperation	Russia did not cooperate
Cui Bono?	High: Russia[53]
Correlation with National Policy	Very strong[54]
Correlation with Physical Force	Very strong[55]

44 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 3.
45 *Ibid.*, 2: "... little or no direct involvement on the part of the Russian government or military."
46 *Ibid.*, 3.
47 Zigfield, "Re-Imposing Totalitarian Information Control in Russia."
48 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 4: "The types of cyber attacks used against Georgia were ... carried out in a very sophisticated manner."
49 *Ibid.*, 4: "The types of cyber attacks ...were limited to denials-of-service and website defacements..."
50 As with Estonia, though commercial targets were attacked, there was little chance for commercial gain, though this should not weigh heavily in our attribution.
51 After researching Russian hacker sites, Project Grey Goose was unable to find any evidence for Russian state support or assistance. Greylogic. "Project Grey Goose Phase I Report.
52 The Russian government made repeated public statements (as part of their invasion). Hackers also left a public chain of comments where they exchanged target lists.
53 There were no other nations or groups that obviously benefited from attacking Georgia or were in an existing crisis.
54 The Russian government made their policy clear when they invaded and did not try to restrain any cyber attacks.
55 *Ibid.*, 3. Most importantly, there was a direct military invention, but also the "...organizers of the cyber attacks had advance notice of Russian military intentions."

For this analysis of Georgia, here are a few analytical elements from the middle of the spectrum of state responsibility:

4. State-encouraged. Third parties control and conduct the attack, but the national government encourages them as a matter of policy.

5. State-shaped. Third parties control and conduct the attack, but the state provides some support.

6. State-coordinated. The government coordinates third-party attackers, such as by "suggesting" operational details.

7. State-ordered. The state directs third-party proxies to conduct the attack on its behalf.

There is weighty evidence in several categories that implies the Russian state provided active assistance. Thus, the attack was clearly not just encouraged but directly supported. One analyst, through direct access to the relevant log files and interviews, concluded that the cyber attackers were tipped off before the military operation, and that "the primary objective of the cyber campaign was to support the Russian invasion..."[56] This implies enough connection with the attackers for the government to suggest targets and timing.

However, there seems to be little evidence that the groups involved were under *direct* orders regarding what to attack and when, so the attacks were likely not state-ordered. Accordingly, the evidence suggests with ***moderate confidence*** **that the attacks on Georgia were *state-shaped or state-coordinated* by the Russian government.** There is not enough reliable evidence at this point to say the attacks were fully state-ordered.

56 Bumgarner and Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 3 and 6.

Here is the comparable analysis for Stuxnet:

Table 6: Analysis of the Stuxnet Cyber Attacks

Analytical Element	Assessment
Attack Traced to Nation	Not applicable[56]
Attack Traced to State Organizations	Not applicable [57]
Attack Tools or Coordination in National Language	Partial[58]
State Control over the Internet	Not applicable[60]
Technically Sophisticated Attack	Highly[61]
Sophisticated Targeting	Highly[62]
Popular Anger	Low[63]
Direct Commercial Benefit	Low[64]
Direct Support of Hackers	Not applicable[65]
Correlation with Public Statements	Very High: US and Israel[66]
Lack of State Cooperation	Possible: US[67]
Cui Bono?	High: US, Israel[68]
Correlation with National Policy	High: US, Israel[69]
Correlation with Physical Force	Moderate: US, Israel[70]

57 Because Stuxnet was inserted by removable media, there was no clear trace, as there is for Internet-based disruptive attacks.
58 Again, there was no traceable network path.
59 More important than language, there were cultural artifacts perhaps pointing to Israel. However, sometimes such artifacts can be misleading and support confirmation bias. For example, a string of numbers can be assigned some cultural significance if, for example, they correspond to a date, which happens to support the analyst's existing theory.
60 There were no external networks involved, so network control is not applicable.
61 Multiple sources (see the chapter on Stuxnet in this book) describe in great detail the sophistication of Stuxnet, which used several zero-day vulnerabilities with code to target Siemens industrial control systems and required extensive testing.
62 As above, see the chapter on Stuxnet for examples of how tightly targeted Stuxnet had to be to only disrupt Iranian nuclear enrichment and nothing else.
63 Some citizens may be upset at Iran's enrichment plans, but none possessed the needed capability.
64 Theoretically, a competitor of Siemens or a consultant, seeking hefty fees to fix the Iranian's malfunctioning centrifuges, might have a commercial motive, but this is a thin theory, given the tool's capability.
65 Stuxnet was too sophisticated to be a hacker attack, so any nation's support of hackers is not applicable.
66 The disruption of the Iranian program was a critical foreign policy goal of these two countries—and few others. In addition, detailed press reports described in great detail the US and Israeli involvement. These were stories which demonstrated clear access to senior officials and were denied by both countries.
67 Anecdotally, the author has heard that the US government had asked US cybersecurity companies to ignore Stuxnet as much as they could.
68 The disruption of the Iranian program was a critical foreign policy goal of these two countries—and few others. Few other nations would benefit anywhere near as much.
69 It was such a priority that both nations had publicly considered military options, such as military strikes to delay the program, as Stuxnet did.
70 There was no ongoing physical crisis, but as noted above, both Israel and the United States had discussed plans for military strikes to delay the Iranian program.

The extremely high sophistication of the tool, and the precision and select targeting help to rule out the theory that rogue state actors or non-state adversaries were responsible, even with government help. The attack seems with high confidence to be state-executed: a state conducts the attack using cyber forces under their direct control.

Using a similar analytical process as used for the Estonian and Georgian assaults, and a preponderance of evidence, it is difficult to come to any other conclusion than that there is ***medium confidence*** **that Stuxnet was a** ***state-executed attack*** **by the United States and/or Israel**. And indeed, press reports, not refuted by either government, implicate both. Some analysts pointed the finger at other nations, including Russia and China, but these seem to be "just-so stories," grasping at a few straws of evidence but ignoring the weight of other evidence.

This assessment is not "high" confidence. Senior US officials in off-the-record discussions with the author have made comments hinting that analysts "should not believe everything they believe in the media," suggesting that the evidence implicating the United States is not as credible as it may seem. If so, then US officials should be clear in order to clear the historical record.

There is only twenty-five years of the history of cyber conflict, yet this is enough to identify clear lessons and emerging norms. In time, the interpretations presented here will be either reinforced or possibly refuted. But the world needs more historians, more researchers, and analysts of all types to join in and examine this history, to make their own discoveries and identify their own lessons.

JJH

Assessment Summary

Estonia:

- High confidence that the attacks on Estonia were at least encouraged by the Russian government

Georgia:

- High confidence that the attacks on Georgia were at least ignored by the Russian government
- Moderate confidence they were state-shaped or state-coordinated by the Russian government

Stuxnet:

- Medium confidence that Stuxnet was a state-executed attack by the United States and/or Israel

Appendices

Appendix 1: Glossary

- **Advanced Persistent Threat**: A group, often but not always tied to a government, with the intent and capacity, backed by very significant resources, to effectively and consistently target a specific entity. The APT knows what it wants and has resources to keep going after it from multiple directions, compared to typical hacker groups which only target poorly defended targets. The APT was first well described publicly in the 1991 report, Computers at Risk, by the US National Academies of Science as the "high-grade threat."

- **Advanced Research Projects Agency Network** (ARPANet): An operational packet switching network that was created in 1969 with funding from US military's Advanced Research Project Agency. It was the precursor to the modern Internet.

- **Botnet**: A collection of computers which have been taken over by a malicious attacker (after an *intrusion*) who controls their collective actions with another set of computers, called "botnet herders" or "command and control servers. Botnets can be rented out to raise money for the attacker or can be used to send spam, engage in fraud, or conduct *DDoS attacks*.

- **Comprehensive National Cyber Initiative** (CNCI): The still-classified CNCI was established by National Security Presidential Directive 54/Homeland Security Presidential Directive 23 by President Bush in January 2008 to focus efforts on 12 initiatives, largely focused on defending US government networks.

- **Computer Emergency Response Team** (CERT): A team of people to respond to computer or network outages on behalf of their organization or country. Their exact duties and structure vary between organizations, but typically a CERT will look for threats and patch *vulnerabilities*, develop plans to deal with outages or malicious attacks, and coordinate the response. The first CERT was created in November 1988 at Carnegie Mellon University at the behest of DARPA as a result of the *Morris Worm*.

- **Computer Network Attack** (CNA): A term from the US Department of Defense for an attack done through a network of computers that either disrupts, denies, degrades, or destroys another computer's information or the computers or networks themselves. The term does not include espionage or theft of information (which would be CNE) so long as no information or systems are destroyed.

- **Computer Network Defense** (CND): A term from the US Department of Defense for actions taken to resist attempts to steal, copy, infiltrate, read, disrupt, deny, degrade,