INTERNATIONAL CYBER INCIDENTS:

LEGAL CONSIDERATIONS

Eneken Tikk
Kadri Kaska
Liis Vihul

2010

Contents

ESTONIA 2007

April-May

I Background of the incident

Political context of the incident

On April 26 and 27 of 2007, Estonia witnessed two nights of unprecedented street riots in the centre of Tallinn, its capital, by youth groups mostly of ethnic Russian origin.[1] The riots had broken out in response to the government decision to remove a Soviet-era Second World War (WWII) memorial, a decision which had been accompanied by intense vocal opposition by the government of Russia[2] and by a series of propagandistic articles in the Russian and international media[3], accusing Estonia of "glorifying Nazism" and "rewriting history".

The memorial in question, the centrepiece of which was a two-metre-high bronze soldier, had been erected in central Tallinn in 1947 as a memorial to the victory of the Soviet Army over Nazi Germany in WWII.[4] While in the early 1990ies many Soviet-symbol statues and memorials throughout Estonia were removed, the Bronze Soldier, as a rather neutral example of the Soviet-era memorials, remained intact, and for years it stood at a small park next to a central intersection without causing concern. On WWII-related holidays formerly celebrated by the Soviet Union, those commemorating their

1 Estonia has a sizeable ethnic Russian minority: out of the population of 1,34 million, 344 000 are of ethnic Russian origin. (Statistics Estonia. Statistical Database. Population by Sex, Ethnic Nationality And County, 1 January 2007. pub.stat.ee/px-web.2001/Dialog/statfile1.asp). Within this minority, different groups with various levels of integration into the Estonian society exist. A large percentage holds Estonian citizenship, speak the Estonian language, and consider Estonia as their homeland. Some are citizens of the Russian Federation, of which a number still accept the constitutional order of the Republic of Estonia. Some, however, consider the collapse of the Soviet Union a historical mistake and desire the restoration of Russian dominion over the territory once under Russian control.

2 Among others, the foreign minister of the Russian Federation, Sergey Lavrov, who issued a statement calling the decision „a blasphemy' and threatened 'serious consequences'. *See* Socor, Vladimir. 'Moscow stung by Estonian ban on totalitarianism's symbols'. Eurasia Daily Monitor, The Jamestown Foundation, 26 Jan 2007. Available at http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=32427.

3 E.g. Kosachev, Konstantin. 'An insult to our war dead'. The Guardian, 6 Mar 2007. Available at http://www.guardian.co.uk/commentisfree/2007/mar/06/comment.secondworldwar

4 Kaasik, Peeter. 'Common grave for and a memorial to Red Army soldiers on Tõnismägi, Tallinn. Historical statement'. Estonian Foundation for the Investigation of Crimes Against Humanity, 2006. Available at http://www.valitsus.ee/brf/failid/ajalooline_oiend_2006_en.pdf

losses in war laid flowers on the site. However, in recent years, these events increasingly began to turn into more provocative gatherings of groups which were openly hostile towards the Estonian state, and when conflicts arose out of a case where a person carrying an Estonian flag was physically attacked by the gatherers, the area was taken under heightened police supervision.[5] As the site increasingly became a rallying point for national extremists, a public debate arose on the removal of the memorial, along with relocation of the adjoining war graves.

In the early spring of 2007, the government of Estonia announced the start of preparatory works for the excavation of the war graves, reburial of the bodies to a military cemetery, and relocation of the Bronze Soldier memorial.[6] On April 26, the memorial site was fenced and covered, and preparations for excavations began.

On the evening of April 26, about a thousand people gathered at the memorial site to demonstrate their dissent against the removal of the monument. In later hours, the initially calm protest escalated into violence against the police and later on into street riots with extensive looting and vandalising of buildings and other property in central Tallinn, as well as in the city of Jõhvi north-east of the country. Police arrested 1300 people; about a hundred were injured in the riots, and one person died. The estimated amount of damage directly caused by the street riots was about 70 million kroons (about €4.5 million).[7] The government made a quick decision to move the statue earlier than initially announced, and during the night of April 27, the statue was taken to an unannounced location, and later established at the Tallinn Military Cemetery on April 30.[8]

The decision of relocation set off days of angry protests by Nashi activists in front of the Estonian embassy in Moscow[9] and resulted in physically attacking the Estonian ambassadors at a press conference.[10]Riots in the streets of Tallinn turned into "rioting" in cyberspace when in the late hours of Friday, April 27, web pages of Estonian government institutions and news portals came under a wave of cyber attacks. Attacks against both public and private sector websites lasted, in phases of varying intensity, for more than three weeks; beginning to to subside by May 19 with the overall calming down of political tensions between Estonia and Russia over the Bronze Soldier issue. Some aftermath was still observable at the end of May 2007.[11]

Estonia as an information Society

To understand the significance that the the spring 2007 cyber attacks had against the Estonian governance and society as a whole, the role of information and communications technology needs a few introductory remarks.[12]

The evolution of information society services in Estonia

The small size of the population (1.3 million inhabitants), limited resources, and the low population density have challenged Estonia to look for efficient means to provide public services to its residents without requiring excessive resources from the state.

The advance of Estonia as an e-State dates back to the mid-1990s. The first entities to introduce and promote Internet-based service solutions were commercial banks, who were eager to gain market advantage and to reach the

5 'Politsei viis Eesti lipu lehvitaja minema'. Delfi.ee, 9 May 2006 (*In Estonian*). Available at: http://www.delfi.ee/news/paevauudised/eesti/article.php?id=12845410

6 Rand, Erik. 'Ansip: pronkssõdur viiakse Tõnismäelt minema'. Postimees, 29 March 2007 (*In Estonian*). Available at: http://www.epl.ee/artikkel/380087

7 Ojala, Agnes. Pronksiöö hinda mõõdetakse sadades miljonites. Äripäev 10.07.2007. (*in Estonian*)

8 Pronkssõdur avati taas rahvale vaatamiseks. Postimees Online, 30 April 2007. (*in Estonian*) Available at http://www.postimees.ee/300407/esileht/siseuudised/258058.php

9 Arnold, Chloe. 'Russian Group's Claims Reopen Debate On Estonian Cyberattacks.' RFE/RL, 30 March 2009. Available at: http://www.estemb.org/news/aid-2526

10 Myers, Steven Lee. 'Youth Groups Created by Kremlin Serve Putin's Cause'. New York Times, 8 July 2007. Available at: http://www.nytimes.com/2007/07/08/world/europe/08moscow.html?_r=1

11 Landler, Mark; Markoff, John. 'In Estonia, what may be the first war in cyberspace.' International Herald Tribune. 28 May 2007. Available at http://www.iht.com/articles/2007/05/28/business/cyberwar.php

12 Data provided below is as of 2007, to reflect the situation within the timeframe of the cyber attacks. Where available, data references as of end-2008 are given for comparison.

scarcely populated rural areas.[13] High-quality IT solutions in other industries have followed since then. Internet banking has become prevalent (in 2007, 95% of all banking operations were carried out electronically[14]). Mobile solutions such as mobile parking and mobile public transportation tickets have evolved and gained popularity (m-parking constituted more than 50% of the total income gathered from parking fees in major cities in 2005).[15] There are a number of success stories in the Estonian ICT sector, to name Skype, Regio[16] and Mobi Solutions[17] as a few.[18]

For nearly a decade, it has also been an overarching governance policy to use information technology to increase public sector administrative capacity and to ensure an innovative and convenient living environment for the citizens. The legislative ground for the widespread government-to-citizen e-service use was laid by the 2000-2002 administrative law reform, whereby electronic operations were made equal to written operations in administrative procedure.[19] Digital signatures had already been constituted the same legal consequences as a hand-written signatures in 2000.[20]

Internet access and infrastructure

By 2007, 98% of Estonian territory was covered with Internet access: fixed line, broadband, WiMax, WiFi, and CDMA[21] mobile wireless Internet access solutions.[22] The Internet reaches most of the country's territory, omitting only some small areas because of landscape peculiarities unfavourable for radio transmission. Mobile phone penetration was nearing 100% in 2007[23].

Nearly 50% of the population 16-74 years old was using the Internet in 2007; households having personal computers at home comprised 53% and those having access to the Internet at home, 48%.[24]

Government e-Services

With the creation and development of the national population registry in 1992 began the era of governmental digital databases and state information systems in Estonia. By 2007, state information systems and databases had been developed into a nationwide state information system with corresponding functional infrastructure that enables service access on the principle of "one stop shopping".[25]

In 2007, the state information administration system consisted of more than 150 public sector information systems, which altogether provided more than 1,000 different electronic services. More than 450 public sector organizations and 30,000 entrepreneurs used the data exchange layer[26] (the "X-road") each day via the State

13 Tikk, Eneken; Oorn, Reet. 'Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism.' *In* 'Responses to Cyber Terrorism'. COE DAT, 2008. Pp. 89-103;

14 In end-2008, there were 1,6 million e-banking clients, and over 98% of transactions concluded online. *See* 'Pankadel on üle 1,6 miljoni internetipanga kliendi.' *Delfi Online*, 8 Jan 2009 (*in Estonian*). Available at http://www.delfi.ee/news/eesti/eesti_uudised/article.php?id=20829300.

15 Arthur D. Little Global M-Payment Update 2005. Available at: http://www.3mfuture.com/articles_epayment/Global_M-Payment-Report_Update_Arthur_D_Little_2005.pdf. P. 17.

16 A provider of various GIS and mobile positioning solutions

17 A developer of different m- applications and m-solutions

18 Talihärm, Anna-Maria. 'Estonia 2007: A Possible Model For Cyberterrorism?' Stockholms Universitet, 2008.

19 Administrative Procedure Act (RT I 2001, 58, 354), passed 6 June 2001, entered into force 1 January 2002. *See* Art 5 section 6; Art 14, Art 25-27, Art 55. An unofficial English translation is available at http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=et&sk=en&dok=X40071K3.htm&query=haldusmenetluse&tyyp=X&ptyyp=RT&pg=1&fr=no.

20 Digital Signatures Act (RT I 2000, 26, 150), passed 8 March 2000, entered into force 15 December 2000. *See* Art 3. An unofficial English translation is available at http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=et&sk=en&dok=X30081K5.htm&query=digitaalallkirja&tyyp=X&ptyyp=RT&pg=1&fr=no

21 Code Division Multiple Access (CDMA), a mobile digital radio technology standard.

22 Käo, Merike. 'Cyber Attacks on Estonia: Short Synopsis'. 2007. Available at http://doubleshotsecurity.com/pdf/NANOG-eesti.pdf. P. 4.

23 By end of 2008, this number exceeded 130%. (Data provided by the National Communications Board/Communications Division of the Estonian Competition Authority.) The figure reflects the number of active SIM-cards per population.

24 Implementation Plan 2007-2008 of the Estonian Information Society Strategy. Available at http://www.riso.ee/en/information-policy/policy-document/implementation_plan

25 Tikk, Oorn, *supra* note 13.

26 The data exchange layer, which constitutes the major part of the X-Road system, integrates the databases through user interfaces to a common network and enables the user, within the limits of his/her authority, to search data from national databases that have joined the system.

Portal *eesti.ee*, and over 500,000 citizens had experienced using public sector e-services via the X-road. The number of individuals having given digital signature had reached 70,000 unique signatories by 2007. [27]

In the year 2008, 80% of natural persons' income declarations were submitted electronically.[28] In local government council elections held in October 2005, Estonia was the first country in the world to use Internet voting.[29] About 90% of the performers of high school state examinations received their exam results via SMS in the 2007 state exams.[30]

Over time, more and more government-to-consumer services have moved online in Estonia, while their on-paper provision has increasingly ceased. Consultation and assistance are provided by the state to people that lack the necessary equipment or skill to use online services.[31]

The high availability of public e-services and wide Internet accessibility that the Estonian population enjoys have, as a negative side effect, also made the country a more attractive target for cyber attacks. The dependency of the population on easily accessible online services has made the society more vulnerable to large-scale disruptions in the availability of Internet access.

II Facts of the case

Phases and timeline of the attacks

Cyber attacks started in parallel to rioting on streets in the late hours of Friday, April 27, when web pages of Estonian government institutions and news portals came under a wave of cyber attacks. Estonian e-services and information infrastructure were hit in varying degrees of intensity until the end of May, when the political tensions between Estonia and Russia over the Bronze Soldier issue finally started to calm down.

The attacks had two distinctly different phases, each consisting of several waves of elevated intensity. The first phase took place from April 27 to 29 and was assessed to have been emotionally motivated, as the attacks were relatively simple and any coordination mainly occurred on an *ad hoc* basis. The first phase was followed by the main, co-ordinated attack phase lasting from April 30 to May 18, which was much more sophisticated, and where the use of large botnets[32] and professional coordination was noticed. Notably, clear correlation was observed between politically significant dates and intensification of attacks.

Phase I – emotional response (April 27 to 29)

The first attack against government websites was reported to have hit in the late hours of 27 April 2007.[33] Also attacked in the early days were online media outlets carrying news about the street riots and the overall political situation.

Initially, attacks were carried out by relatively simple means, therefore earning the label of "cyber riots"[34]. In various Russian-language Internet forums, calls and instructions were presented to launch *ping* commands (simple commands to check the availability of the targeted computers) with certain parameters on the MS Windows command line.[35] Later on, executable .bat files were made available for users to copy onto their computers and then launch to carry out automated ping requests.[36] This would amount to simple denial of service

27 Tikk, Oorn, *supra* note 13.
28 *Id.*
29 EurActiv. 'Estonia first country in the world to introduce internet voting'. 12 October 2005. Available at http://www.euractiv.com/en/egovernment/estonia-country-world-introduce-internet-voting/article-145735
30 Tikk, Oorn, *supra* note 13.
31 *Id.*
32 The nature of a botnet is explained under the section 'Intensity and duration of the attacks' of this paper. For definition, see also the *Abbreviations and Glossary* section.
33 Almann, Lauri. Presentation at the Conference Board of Canada conference 'Cyber Security: Proactive Defence of Critical Systems and Information'. 5 Nov 2008.
34 The title given to the initial phase of the incident by Hillar Aarelaid, head of CERT Estonia. *See* Finn, Peter.' Cyber Assaults on Estonia Typify a New Battle Tactic,' Washington Post, 19 May 2007. Available at http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html
35 *Id.*
36 Randel, Tarmo. CERT Eesti tegevuse aastakokkuvõte (CERT-EE Annual Report; *in Estonian*). Estonian Informatics Centre, 2007; Evron, Gadi. 'Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War'. *Georgetown Journal of International Affairs*, Winter/Spring 2008, p 121-126.

(DoS)[37] attacks; however, being coordinated, they were effective in disturbing their targets. Attacks were also coordinated via Internet Relay Chat (IRC).[38]

Pinging was soon followed by malformed web queries, which were massively used mainly against the websites of the government and media outlets – this already implied the use of more specific means designed for attack.[39]

As a generalisation, though, the initial attacks on April 27 and 28 were simple, ineptly coordinated and easily mitigated.

Phase II – Main Attack (April 30 to May 18)

In the second phase, more sophisticated and better-coordinated attacks appeared in four major waves outlined below. Compared to the initial emotional response, phase II was also clearly characterised by use of larger botnets.[40]

In addition to the higher level of sophistication of coordination and attack, the initial model of using Internet forums to distribute instructions and lists of targets to attack was still employed. The instructions were mostly very simple, thus not requiring advanced technical knowledge or skill to follow; a computer with an Internet connection was sufficient to participate. Calls were issued to schedule attacks for specific timings in order to generate greater simultaneous volume of queries for higher effect against targets.[41] Discussions about how to fund the rental of server farms[42] and botnets for distributed denial of service (DDoS)[43] attack were also present.[44]

The Domain Name Servers (DNS) and routers run by Elion[45] were repeatedly attacked throughout the period between April 30 and May 18, causing temporary service disruptions.[46] Outside the peak days described below, network traffic continued to be above the normal level throughout this period. In the majority, the attacks were manageable, but some sites were affected and remained inaccessible for periods of time.

First Wave (May 4)

During the night of May 4, DDoS assaults continued against websites and DNSs, while showing remarkable intensification and precision in concentration[47], which indicated the use of botnets. Attackers covered their tracks by various means: by using global botnets, by routing their attacks through proxy servers in other countries (including those in NATO countries) and likely by spoofing their IP addresses[48].[49]

Second Wave (May 9-11)

Yet another increase in attacks was expected for May 9, 2007. May 9 is the day celebrated annually as Victory Day in Russia, a national holiday which remembers the defeat of Nazi Germany in World War II, and thus of direct relevance to the Bronze Soldier controversy.

As anticipated, the DDoS attacks increased by

37 DoS – a Denial of Service attack, where a server is overloaded with irrelevant queries or information packages originating from the same terminal. Technical terms are explained in *Abbreviations and Glossary* of this book.
38 Ottis, Rain. Overview of Events, 30 April 2007. CCD COE Activation Team, TDCCIS.
39 Randel, *supra* note 36.
40 *Id.*
41 Ottis, Rain. Overview of Events, 2 May 2007. CCD COE Activation Team, TDCCIS.
42 A group of networked servers, housed in one location, to streamline internal processes by distributing the workload between the individual components of the farm. For a more detailed explanation, see *Abbreviations and Glossary* of this book.
43 A denial-of-service attack (DoS) occurs when large number of requests are directed to a target URL. The requests occur so quickly that the Web server cannot respond and the site becomes inaccessible. A distributed denial-of-service attack (DDoS) occurs when hundreds or thousands of compromised computers are enlisted. For a more detailed explanation, see *Abbreviations and Glossary*.
44 Ottis, *supra* note 41.
45 Elion Ettevõtted AS is the leading player on fixed electronic communications services markets in Estonia.
46 Cyber attacks against the Republic of Estonia. 10 May 2007. An overview by the Cooperative Cyber Defence Centre of Excellence project team.
47 Overview of Events, 4 May 2007. CCD COE Activation Team, TDCCIS.
48 IP address - the unique 32 bit number assigned to each computer connected to the Internet and used by the TCP/IP protocol to route packets of data to their destinations. For a more detailed explanation, see *Abbreviations and Glossary*.
49 Overview of Events, *supra* note 47.

about 150% at 23:00 EET[50] on May 8 (beginning of May 9 according to Moscow time)[51], and lasted throughout May 9 and 10, then ending abruptly. On May 9, the attacks shut down up to 58 sites at once.[52] This wave of attacks mostly targeted government websites (including official communications channels of the government)[53]; in total intensity however, the attack remained lower than those that had taken place in previous weeks.[54]

The banks experienced more sustained DDoS attacks from May 9 to 11, with the web service of the largest commercial bank of Estonia, Hansapank, being unavailable for customers for ca 1,5 hours on May 9 and for another two hours on May 10.[55]

Third Wave (May 15)

Strong DDoS attacks (via a large botnet of about 85,000 hijacked computers as reported by the Estonian Computer Emergency Response Team [CERT-EE]) against the websites of government institutions took place from noon until midnight on May 15. Since network capacities had already been increased in response to the earlier attacks, the heightened amount of traffic did not pose significant problems.[56]

The web portal of SEB Eesti Ühispank, the second largest commercial bank, was offline for ca 1.5 hours, and the restoration of service for customers outside of Estonia took longer still. There were lesser incident reports from other banks.[57]

Fourth Wave (May 18)

Another strong DDoS attack against governmental websites occurred. Banks continued to experience a diminished level of interruptions even after that date.[58]

Means and types of attacks against Estonia

The means of attack used in the April-May 2007 events included denial of service (DoS) and distributed denial of service (DDoS) attacks, defacement of websites, and large amounts of comment and email spam. Public propaganda, distributed on different Internet forums, and dissemination of attack instructions were employed to encourage, coordinate and aid in carrying out the attacks.

DoS and DDoS attacks

In the early few days of the Estonian cyber incident, most of the attacks consisted of denial of service (DoS) and distributed denial of service (DDoS) attacks which resulted in the attacked websites becoming inaccessible.

A denial-of-service attack is a concerted malevolent effort to deny access to any electronic device, computer, server, network, or Internet resource by its intended users.[59] This can be accomplished in numerous ways; ping-flooding, UDP flood and malformed queries were mainly used in the case of the Estonian attacks. Malformed GET queries, SYN floods, and the so-called 'ping of death' method were also used.[60]

The effect of the DDoS attacks was more severely noticed by users outside of Estonia, as a large amount of foreign queries were cut off in order to cope with the excessive traffic and to filter out genuine queries.[61]

As the attacks progressed, massive distributed

50 Eastern European Time (EET), GMT+2, which, notably, is one hour behind the Russian Standard Time (GMT+3).
51 Ottis, Rain. Overview of Events, 9 May 2007. CCD COE Activation Team, TDCCIS.
52 Nazario, José. 'Estonian DDoS Attacks - A summary to date'. Arbor Networks. May 17th, 2007 Available at asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/
53 Randel, *supra* note 36.
54 As demonstrated by data transfer volume graphs recorded by Elion, the major service provider, between 27 April and 11 May.
55 'Hansapanka tabas küberrünne'. Postimees 10 May 2007 (*In Estonian).* Available at http://www.tarbija24.ee/180507/esileht/majandus/259920.php
56 Ottis, Rain. Overview of Events, 15 May 2007. CCD COE Activation Team, TDCCIS.
57 Ottis, Rain. Overview of Events, 16 May 2007. CCD COE Activation Team, TDCCIS.
58 Landler, Markoff, supra note 11.
59 Cyberwarfare: a glossary of useful terms. Stratfor today, 1 March 2008. Available at http://www.stratfor.com/analysis/cyberwarfare_glossary_useful_terms *See* also *Abbreviations and Glossary.*
60 For explanation on the technical terms, see Abbreviations and Glossary.
61 *See section* 'Measures Taken to Cope with the Attacks' of this paper.

denial of service (DDoS) attacks were targeted against key governmental and private sector web sites, selecting some critical information infrastructure targets (DNS) while using a wide array of offensive techniques. At their peak, the amount of Internet traffic from outside of Estonia, targeting governmental institutions, was nearly 400 times higher than its normal rate. According to Arbor Networks, a global network security solutions R&D corporation that observed the Estonian cyber attacks and provided their observations for part of the attack period, 128 unique DDoS attacks were detected on Estonian websites during that period.[62]

Defacement of websites

A hacker succeeded at breaking into the Estonian Reform Party website where they placed a forged "official" apology, signed by Estonian Prime Minister Andrus Ansip.

The apology, in contrast with the language of the rest of the website, was offered in Russian. There were also reports of doctoring of a photo of the Prime Minister Ansip to add a Hitler moustache[63].

Attacking DNS servers

A more dangerous trend was attacking the DNS servers managed by Internet Service Providers. Repeated attacks against DNS and routers run by Elion were observed between April 30 and May 18. Some of the attacks were successful in the short term, temporarily disrupting DNS services in parts of the country.[64]

Other Types of Attack

Heightened use of mass unsolicited e-mail was observed against government e-mail servers and individual e-mail accounts. Due to public policy applicable since 2001 to publish contact addresses for all public service employees on their entities' websites, these addresses were an easyMass spread of comment spam by robots posting on internet forums and news sites also occurred. These had varying effects, but in general, most systems were able to withstand the attacks.[65]

Attack targets

The prime targets (and also those that experienced major effect) were information distribution channels of both the government and the private sector, and business sector websites, specifically, the banks. The work of vital databases, systems or registers of the public and private sector was not disrupted, but there were attacks directed at the national Internet infrastructure. Also, the common emergency number 112 was targeted so that calls were briefly blocked.[66]

The targets for cyber attack were mainly fourfold (discussed in more detail in following subsections):

- servers of institutions that are responsible for the Estonian Internet infrastructure;
- governmental and political targets;
- services provided by the private sector;
- personal and random targets.

Notably, traditional critical infrastructure objects, such as information systems supporting transportation and energy systems, were not targeted.

Internet infrastructure providers

CERT-EE reported several occasions of attacks against the Estonian Internet infrastructure and information systems, both governmental and commercial.[67]

Among servers especially pointed out as targets (with instructions given on how to attack) were the national DNS run by the Institute of Chemical Biology and Physics (the institution responsible

62 Nazario, supra note 52.
63 Finn, Peter, *supra* note 34.
64 Cyber attacks against the Republic of Estonia, *supra* note 46.
65 *Id.*
66 Estland im Visier: Ist ein Internetangriff der Ernstfall?. Frankfurter Allgemeine Zeitung, 18.06.2007, Nr. 138 / Seite 6. (in German). Available at: http://www.faz.net/s/RubDDBDABB9457A437BAA85A49C26FB23A0/Doc~E7CCF88CEFB6F467BB8D75A400C07B959~ATpl~Ecommon~Scontent.html; Ottis, Rain. Overview of Events, 7 May 2007. CCD COE Activation Team, TDCCIS.
67 Tiks, Oliver (ed). 'Küberrünnakuid tõrjuvad sajad spetsialistid' (*In Estonian*). Postimees Online, 2 May 2007. Available at http://www.tarbija24.ee/120507/esileht/siseuudised/258274.php

for Estonian domain name administration); EENet, which administers the core Internet servers for the Estonian governmental and educational institutions; and also ISP-operated DNSs (a full list of country DNS targets, identified both by their URL and by IP address, was distributed over a Russian-language web forum).[68]

Governmental and political targets

Among governmental and political websites, those attacked were[69]:

- Estonian constitutional institutions:
  - Government,
  - Prime Minister,
  - President,
  - Riigikogu (the Parliament),
  - State Audit Office.
- Governmental institutions:
  - all ministries (state departments) except for the Estonian Ministry of Culture;
  - state agencies (e.g. the Estonian Police Board);
- Reform Party, the website of the leading coalition party.[70]

CERT-EE confirmed that persistent attacks against the official communications channels of the Estonian government lasted throughout the period between April 27 and May 9.[71]

Commercial Services

E-banking services of Hansapank and SEB Eesti Ühispank, two of the largest banks that, combined, controlled about 75-80% of the total Estonian banking market, were attacked on various occasions between the period of May 9 to 15.[72] Diminished interruptions continued even after that date. Hansapank's e-banking service had to be shut down from 1,5 to 2 hours on two occasions (May 9 and 10)[73], SEB Eesti Ühispank's online banking service was offline for 1,5 hours on May 15. Both banks reported having to restrict access to customers located abroad in order to cope with the massive amounts of queries originating from outside of Estonia. Considering that the use of e-banking services is almost exclusive in Estonia (in 2007, the share of electronic transactions amounted to about 95-97%), the effect was significant on large parts of the society and economic activities were hindered throughout the entire country. No entities have publicly announced the size of their cyber losses though.[74]

At least three major Internet Service Providers – Elion Ettevõtted, Elisa Andmesideteenused, and Starman – experienced DDoS attacks against their servers.

Three of Estonia's six largest news organisations and news portals (including Postimees.ee, Delfi, EPL Online, Baltic News Service) were also affected. The country's three mobile network operators experienced slight disruptions.[75]

A web hosting service provider (Zone.ee) and a directory service provider (ee.ee) were attacked by DDoS, possibly because these were errone-

68 Reference to the original site has been withdrawn from this paper to avoid being a redistribution point. Contact the authors for reference. For an explanation on the abbreviations and terms used, see *Abbreviations and Glossary*.

69 Rantanen, Miska. 'Virtual harassment, but for real.' Helsingin Sanomat International Edition, 6 May 2007. Available at http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868; Hyppönen, Mikko. 'Unrest in Estonia'. April 28, 2007. http://www.f-secure.com/weblog/archives/00001181.html; Ottis, *supra* note 66.

70 A 20-*year*-old Tallinn resident Dmitri Galushkevich was convicted for attacking the Reform Party website by DoS attack. (*See* 'Rahutuste ajal Reformierakonna kodulehte rünnanud noormees sai trahvi.' (*In Estonian)* Postimees, 23 Jan 2008. Available at http://www.postimees.ee/250108/esileht/krimi/307821.php.) As of August 2009, this is still the only conviction for any of the cyber attacks under discussion.

71 Randel, *supra* note 36.

72 'Küberründed ei ole vaibunud'. Postimees, 10 May 2007 (*in Estonian*). Available at: http://www.tarbija24.ee/110507/esileht/krimi/259961.php; 'Hansapanka tabas küberrünne'. *supra* note 55.

73 Weiss, Michael. Here Come the Cyber Wars. Are We Ready? Reason.com August 17, 2007. http://www.reason.com/news/show/121896.html

74 In 'Here Come the Cyber Wars. Are We Ready?' Reason.com 17 August 2007. (Available at http://www.reason.com/news/show/121896.html), Michael Weiss reports of the expense of one 1-hour break being at least $1 million. The reliability of this figure is however, not verified; it also only relates to a fraction of the total service disruption.

75 Ottis, *supra* note 66.

ously taken for state information channels.[76]

Origin of the attacks

According to CERT-EE, the attacks mainly, although not exclusively, originated from sources outside of Estonia.[77] The malicious purpose of the traffic was evident from the commencement of the incident, according to CERT officials – by the nature and setup of the queries, it was apparent that the unusually high traffic flow was not merely caused by a sudden and unexpected increase in foreign interest towards information published on Estonian websites.[78]

Information collated by Arbor Networks showed that attacks were sourced worldwide rather than just from a few locations.[79] According to the State Informatics Centre, there were computers involved from 178 countries[80].

A substantial part of the attackers were crowds affected by nationalistic/political emotions who carried out the attacks according to the instructions provided in Internet forums and websites.[81] As the tension around the Bronze Soldier subsided, this type of protesters quieted down, even though some zealous attackers (such as some activists of the *Nashi* movement) were motivated to carry on longer[82]. The switchover from the simple emotional attacks to botnet use was gradual, not abrupt.

Log analyses affirm that the second phase of the cyber attacks involved coordination and resources unavailable to *ad hoc* "regular citizen" protest. As was observed, the second phase attacks had the features of central command and control: they were fairly sophisticated, came in (often precisely timed) waves, and required both financial and intellectual resources.[83]

Particularly in the early "emotional" phase, some attackers were identifiable by their IP addresses. A number of those were Russian, including some cases where the IP address involved in the attack belonged to Russian state institutions.[84] However, Russian authorities denied any involvement[85], and cyber security experts also pointed out the possibility of spoofing attacker addresses and pointed out the lack of "evidence of who is behind the attacks supposedly coming from Moscow".[86]

A few self-proclaimed or self-acknowledged attackers were distinguished: one of them was Konstantin Goloskokov (spelled as Goloskov in some sources)[87], a commissar of the pro-Kremlin Russian youth group *Nashi*, another Dmitri Galushkevich, a young IT student from Tallinn who boasted about successfully attacking the Reform Party's website and who was later convicted for this offence.[88] In March 2009, Sergei Markov, a State Duma Deputy from the pro-Kremlin Unified Russia party, stated that the Estonian attacks had been carried out by

76 Berendson, Risto. 'Küberrünnakute taga seisavad prof*id*.' (*IN Estonian.*) Postimees, 3 May 2007 Available at http://www.tarbija24.ee/120507/esileht/siseuudised/258409.php

77 Randel, *supra* note 36.

78 Tiks, Oliver (ed.) 'Pahatahtlikud küberründed Eesti vastu tulevad välismaalt'. (*In Estonian.*) Postimees Online, 29 April 2007. Available at http://www.tarbija24.ee/110507/esileht/siseuudised/257862.php

79 'Estonian DDoS - a final analysis'. Heine Online, 31 May 2007. Available at http://www.h-online.com/security/news/item/Estonian-DDoS-a-final-analysis-732971.html

80 Clover, Charles. 'Kremlin-backed group behind Estonia cyber blitz'. Financial Times, 11 March 2009. Available at http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?nclick_check=1

81 First calls to attack Estonian sites were discovered on 28 April 2007 at Russian hacker sites and internet forums http://2ch.ru and http://forum.xakep.ru, later on also on http://www.web-dozor.ru and others, complete with target lists and instructions.

82 Ottis, Rain. Overview of Events, 3 May 2007. CCD COE Activation Team, TDCCIS.

83 Kash, Wyatt. 'Lauri Almann: Lessons from the cyberattacks on Estonia'. GCN Interview with Lauri Almann, Estonia's permanent undersecretary of Defence. Government Computer News, 13 Jun 2008. Available at: http://gcn.com/Articles/2008/06/13/Lauri-Almann--Lessons-from-the-cyberattacks-on-Estonia.aspx?p=1. Mr. Almann was a member of the Estonian government crisis management committee at the time of the incident. The crisis management committee is responsible for coordination of all crisis-management related government activities.

84 Traynor, Ian. 'Russia accused of unleashing cyberwar to disable Estonia.' The Guardian, 17 May 2007. Available at http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

85 'Estonia hit by 'Moscow cyber war'. BBC News, 1 7 May 2007. Available at http://news.bbc.co.uk/2/hi/europe/6665145.stm; 'NATO Sees Recent Cyber Attacks on Estonia as Security Issue'. DW staff / AFP / dpa (nda) 26 May 2007. Available at http://www.dw-world.de/dw/article/0,2144,2558579,00.html

86 Millman, Rene. 'DDoS attacks on Estonia 'not from Kremlin''. ITPro. 1 June 2007. Available at http://www.itpro.co.uk/114570/ddos-attacks-on-estonia-not-from-kremlin

87 Yasmann, Victor. Monument Dispute With Estonia Gets Dirty. Russia Report May 8, 2007. Radio Free Europe/Radio Liberty, 8 May 2007. Available at http://www.rferl.org/content/Article/1347550.html; Clover, *supra* note 80.

88 Postimees, *supra* note 70.

his assistant as part of "a reaction from civil society"[89], which confirms earlier information of *Nashi* activists having been part of the attacks, even though the description of methods that were claimed by Markov and Goloskokov only matches part of the attacks experienced.

Measures taken to cope with the attacks

Technical measures

Response to cyber attacks was coordinated by CERT-EE, with the help of system administrators and experts both within and outside of the country. Top Estonian IT specialists from the public and private sectors were engaged on a round-the-clock basis.[90]

The first technical response to the random DoS attacks was to gradually increase the bandwidth of state information system servers (allowing for greater data traffic handling capacity), and to filter out the malicious traffic. By May 9-10, the bandwidth capacity of government networks had been increased to several times above the normal capacity.[91]

Other technical security measures included the application of security patches, firewalling, use of attack detection systems, using multiple servers and/or connections, blocking access, etc. In cooperation with ISPs, the data transmission capacity of incoming connections to Estonia was reduced. This blocked off a part of the attacks, but, as a negative side effect, also part of genuine traffic.[92] As patterns in attacks were distinguished, filtering grew more efficient to block off attacks at the ISP level – both by the Estonian and foreign service providers.[93] Some sites were restored to a "lightweight mode" – e.g. the Police Board that temporarily switched to a simple one-page html-view – to better cope with the amount of incoming queries.[94]

International cooperation

International support was organised by the Ministry of Defence; EU and NATO nations were informed of the ongoing cyber attacks. In response, international cooperation was offered by several nations to limit the attacks originating or passing their respective jurisdictions.[95]

From May 8 to 10, NATO (NCIRC) and US CERT observers visited Estonia, mainly in order to observe the situation, as well as to provide assistance and advice.[96] United States governmental institutions assisted in locating and shutting down sources of attack.[97] Of foreign partners, CERT Finland was especially helpful in providing contacts and assistance in reaching service providers and computer incident response coordination entities of other countries.[98]

As news was published about Estonia cooperating with foreign authorities to locate the cyber criminals and bring them to justice, the number of spontaneous attackers began to diminish.[99]

Effects of the attacks

The cyber effects had both a direct economic and a wider societal effect. As many sectors of commerce and industry rely on ICT infrastructure and electronic communication channels in their daily conduct of business, the overload of e-mail servers, network devices and web servers of internet service providers not only affected large entities such as banks, media corporations, and governmental institutions, but also small and medium size enterprises whose daily business activities were seriously impaired.[100] The

89 Behind The Estonia Cyberattacks. Radio Free Europe/Radio Liberty, 6 March 2009. Available at http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html
90 Tiks, *supra* note 67.
91 Ottis, Rain. Overview of Events, 10 May 2007. CCD COE Activation Team, TDCCIS.
92 Ottis, *supra* note 66.
93 Ottis, Rain. Overview of Events, 14 May 2007. CCD COE Activation Team, TDCCIS.
94 Hyppönen, Mikko. 'Update on the Estonian DDoS attacks.' F-Secure Weblog, 30 April 2007. Available at http://www.f-secure.com/weblog/archives/00001183.html
95 Kash, supra note 83; An Overview of Events, compiled by the CCD COE activation team on 8 May 2007.
96 Ottis, Rain. Overview of Events, 7 May 2007. CCD COE Activation Team, TDCCIS; Ruiz, Maricelle (ed). 'Internet Law - Should We Go To War Over A Massive Cyber-Attack?' Internet Business Law Services, 23 May 2007. Available at http://www.ibls.com/internet_law_news_portal_view.aspx?id=1762&s=latestnews; Finn, *supra* note 34; Traynor, *supra* note 85.
97 Ottis, *supra* note 66.
98 Randel, *supra* note 36.
99 Ottis, *supra* note 66.
100 Randel, *supra* note 36

cyber attacks thus had a perceptible effect to the functioning of domestic economy.[101]

The attacks also had a societal effect. Due to the e-Government reforms of recent years, non-electronic government communication channels and means of dissemination of information have been largely reduced, not to mention the shift in user habits which means that people are unaccustomed to looking for the information elsewhere than online. Because of the unavailability of government websites and the excessive spamming of official e-mail addresses, normal communication with government was impaired for citizens. By law, state authorities are obliged to treat electronically submitted documents or correspondence on equal basis with documents submitted on paper.[102] Ministries and state agencies – being obliged to do so by law[103] – provide detailed information on their services and contacts, as well as information request and application forms on their websites. When the websites closed down and e-mail addresses were flooded with spam, these information and communications channels became inaccessible. Only because the unavailability of government websites was temporary, it can be estimated that cyber attacks on government websites were not critical nor posed significant daily problems for the population in general.

Cyber attacks against online public services provided via the State Portal *eesti.ee* had a discernible effect for certain segments of the population, since these services are widely used for filing tax reports, applying for state benefits and subsidies and for other communication with the government that has a direct practical or monetary significance for the person involved. While the attacks did not cause long-term unavailability of service for users within Estonia, this was the case for those located abroad. It is difficult, if not impossible, to estimate the amount of damages caused to the population; we are only able to offer a conclusion that the unavailability of government websites may have had undesirable effects for parts of the population that went beyond mere inconvenience and also caused material damage or loss.

Last but not least, the attacks also affected the nation's information flow to the outside world.

Large international global/regional media organisations do not have stations or representatives in Estonia. The Estonian government relies on online briefing rooms and online media to distribute information, and these are widely used by the international media. [104] The receipt and dissemination of first-hand information about the Bronze Soldier riots, the siege of the Estonian embassy in Moscow and the cyber attacks was therefore impaired; in fact, local media web outlets and the Estonian government's online briefing room were among the first sites to come under cyber attack.[105] Again, the immediate loss caused by this is difficult to estimate, but the parties involved had to find alternative means of information exchange.

III Legal considerations

What response in law?

As the Estonian cyber attacks gained international attention, attempts were quick in trying to label them in terms of existing legal institutions. Parallels to conventional warfare and terrorism were drawn, and while some Estonian politicians initially uttered emotional statements comparing the attacks to conventional military activity, it was clear to the Estonian authorities that the cyber attacks could – and should – be treated as cyber crime under the applicable Penal Code and investigated in accordance with national law and relevant international agreements. The question of invoking article 5 of the Washington

101 See the discussion under section "Attack Targets" ("Internet infrastructure providers", "Government and political targets", and "Commercial services").

102 Administrative Procedure Act, § 5 (6). An unofficial English translation of the Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40071K3&keel=en&pg=1&ptyyp=RT&tyyp=X&query=haldusmenetluse

103 Public Information Act, § 28. Unofficial English translation of the Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40095K3&keel=en&pg=1&ptyyp=RT&tyyp=X&query=avaliku+teabe

104 Almann, *supra* note 33.

105 See *supra* in "Phase I – emotional response (April 27 to 29)".

Treaty was never seriously considered.[106]

Procedural issues in national law

Identification of the originators of the spring 2007 Estonian cyber attacks was naturally dependent on measures and procedures that were legally permissible. In accordance with the Estonian Surveillance Act, collecting of information concerning data communicated via electronic communications networks – including the fact, duration, manner and form of communication, personal data and location of senders and receivers of such data – is considered a *surveillance activity*, which is strictly available only to surveillance agencies within the limits of their competence and within procedures authorised by law.[107] Unauthorised surveillance, i.e. observation of a person's activities in order to collect information relating to such person, is criminalised and punishable by law.[108] This effectively ruled out the possibility of having the ISPs or CERT monitor and analyse data logs with the objective of identifying particular attackers. Such activities are reserved to law enforcement agencies in investigation proceedings of specific crimes demarcated in the Code of Criminal Procedure (§ § 110–112).

According to the aforementioned provisions of the Code of Criminal Procedure, evidence may be collected by surveillance activities in a criminal proceeding if collection of the evidence by other procedural acts is a) precluded or especially complicated and b) the criminal offence under investigation is, at the minimum, an intentionally committed crime for which the law prescribes a punishment of at least three years' imprisonment. Only in those cases may evidence also be collected by surveillance activities on the basis of an international request for pre-trial investigation assistance.[109]

However, the majority of the criminal acts committed in the Estonian cyber incident failed to meet the 'three years' imprisonment as punishment' criteria. The lawmakers considered computer crimes as crimes directed against the rights and lawful expectations of individual users[110]; such a dimension that the 2007 cyber attacks demonstrated was never foreseen in drafting the Penal Code. The punishment prescribed by law for computer crimes, at the time of the 2007 incidents, was pecuniary punishment or a maximum one year of imprisonment.[111] This put the availability of the one useful surveillance activity – collecting information concerning data communicated via electronic communications networks – out of reach.

For specific computer crimes, procedural law did allow for evidence collecting by a specific type of surveillance activity titled "single inquiry" (defined as "an inquiry for obtaining information specified concerning *a particular* telephone call, a *particular* electronic mail, a *particular* electronic commentary or another communication session related to the forwarding of a single message"[112] [our emphasis]); however, this measure was inefficient to deal with the massive number of DoS and DDoS queries in the 2007 incidents, mainly for the disproportion between the bureaucratic burden contained in procedural requirements and the minuscule potential value derived of this effort. For each single inquiry, all procedural requirements for surveillance activities would have had to be followed – meaning that a reasoned request had to be submitted by the prosecutor to a preliminary investigation judge for the conduct of each surveillance activity, a detailed report had to be drafted on each inquiry, and each such activity was subject to questioning in the later course of proceedings. In other words, single inquiries

106 As expressed by Mr. Jaak Aaviksoo, Estonian defence minister, it was clear that 'At present, NATO does not define cyber-attacks as a clear military action. [...] Not a single NATO defence minister would define a cyber-attack as a clear military action at present.' *See* Traynor, *supra* note 85.

107 These are the Security Police Board, Police and Border Guard Board, the Military Police, the Prisons Department of the Ministry of Justice and prisons, and the Tax and Customs Board. *See* § 12 (1) section 5, § 6 (1) and (2) of the Estonian Surveillance Act.

108 § 137 of the Estonian Penal Code. Penal Code of Estonia (RT I 2001, 61, 364; 2009, 39, 261). An unofficial English text is available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik

109 § 110, 117 of the Estonian Code of Criminal Procedure

110 Sootak, Jaan; Pikamäe, Priit. Karistusseadustik: kommenteeritud väljaanne. 2nd ed. Juura, 2009 (*The authoritative Commentary of the Estonian Penal Code*). Pp 454-457.

111 Penal Code, § § 206-208. For some cases involving severe damages or a previous offence of the same kind, an elevated term of punishment applied.

112 § 110 (1^1) of the Estonian Code of Criminal Procedure

would in all likeliness have produced "a lot of trees, but no forest".

Combining the complications discussed above with the restriction regarding issuing international requests for assistance (as this measure was not legally permissible in those cases where the "single inquiry" was the only surveillance activity permitted) in a situation where attacks were globally sourced from over a hundred nations, and it becomes apparent that the national legal system was not likely to do too well in identifying the perpetrators.

International cooperation in criminal matters

According to article 3 of the Agreement on Mutual Legal Assistance between Estonia and Russia[113], signed in 1993, the states render each other legal assistance that includes procedural activities provided by law and conducted by the party who has received the request. Such assistance, according to Article 3, "includes procedural acts foreseen by the law of the receiving party, such as interrogation of parties, accused and accused at trial, witnesses and experts; expert assessments; inspection by court; transfer of physical evidence; initiating prosecution against the person who has committed a criminal offence; and criminal extradition; recognition and execution of court judgments in civil matters; service and transfer of documents; and transfer of data on the punishment of the accused, requested by the other party". As can be derived from the phrasing of the provision (the list of activities is preceded by the phrase "such as"), the list of procedural activities is not exclusive and can include other procedural acts permitted by the law of the receiving country.

Seeking for assistance in criminal investigations to identify persons that participated in the April-May 2007 cyber attacks, and based on the provisions in the Penal Code referring to computer sabotage, damaging a computer network, and the spread of computer viruses, the Estonian Public Prosecutor's Office submitted a letter rogatory to the Russian Federation on 10 May 2007 in accordance with the aforementioned agreement.[114] The letter rogatory included specific IP addresses and references to web forum users, who were likely located on the Russian territory and whom Russia was asked to assist to identy[115].

In a reply of 28 June 2008, the Russian Federation refused to grant the request, stating that the procedural act requested in the letter rogatory was not foreseen by the mutual legal assistance treaty.[116] According to the reply, the agreement lays down that legal assistance shall be rendered in the framework of procedural actions according to the legal acts of the party who has received the request, but the agreement does not require cooperation in the field of operative surveillance measures (*operativno-rozysknye meroprijatija*) in order to identify a person's location.[117]

Even though the Russian approach to this agreement was formally not ungrounded, refusal was not the inevitable legal solution, considering both earlier cooperation practice with Russia and the practice with other countries with whom identically phrased bilateral agreements apply.[118] According to the prosecutor's office, earlier similarly phrased requests for conducting surveillance activities in criminal proceedings had been met by the Russian Prosecutor's Office, but in the cyber attacks case, the office took a different interpretation to the mutual as-

113 Agreement on Legal Assistance and Legal Relations in Civil, Family and Criminal Cases, signed on 26 January 1993. RT II 1993, 16, 27.

114 'Alustati kriminaalasi küberrünnakute uurimiseks.' Press release by the State Prosecutor's Office 2 May 2007. Available at: http://www.prokuratuur.ee/28707

115 'Küberrünnete korraldajaid ähvardab ELi vahistamismäärus.' BNS, 12 March 2009. Available at: http://www.postimees.ee/?id=93564; Pau, Aivar. 'Venemaa keeldus koostööst küberrünnakute uurimisel'. EPLOnline, 6 July 2007. Available at: http://www.epl.ee/artikkel/392271.

116 Pau, *Id.*

117 'Vene saatkond: Eesti ei saatnud korrektset teabenõuet'. Postimees, 10 May 2007 (*In Estonian*). Available at: http://www.euro.postimees.ee/100707/esileht/siseuudised/viimased_sundmused/271542.php

118 Identical phrasing occurs for example in the bilateral treaties for mutual legal assistance with the Ukraine and Poland. *See* 'Eesti Vabariigi ja Ukraina leping õigusabi ja õigussuhete kohta tsiviil- ning kriminaalasjades'. signed on 15 February 1995, entry into force 07 February 2000 (Published in RT II 1995, 13/14, 63); 'Eesti Vabariigi ja Poola Vabariigi vaheline leping õigusabi osutamise ja õigussuhete kohta tsiviil-, töö- ning kriminaalasjades', signed on 27 November 1998, entry into force 17 May 1996 (Published in RT II 1999, 4, 22).

sistance treaty.[119]

According to Norman Aas, Attorney General of the Estonian Public Prosecutor's Office, criminal cooperation with Russia has been complicated since 2006, when the previous Minister of Justice and Attorney General of the Russian Federation were replaced. Since then, Russia has refused to cooperate in certain aspects stipulated in the mutual assistance treaty, while still granting certain other requests.[120] Specifically, Russia has declared that it will not interrogate a suspect of Russian citizenship nor conduct any other procedural activities directed toward them at the request of another country.[121]

Therefore, in all likeliness, the problematic interpretation of the agreement on mutual legal assistance between Estonia and Russia was not due to a judicial impediment – the ambiguity of the mutual assistance treaty or the letter rogatory being ill-formed – but rather depended on pragmatic will (or lack thereof) to cooperate.

The prosecution of cyber attacks originating from Russia has stood at a standstill since the Russian refusal letter. The Estonian Prosecutor's Office holds that the letter rogatory applies and should be treated in accordance with the applicable agreement between the two countries.[122]

Beside the problematic cooperation with Russia, another specific obstacle that complicated criminal proceedings was the issue that the attackers had purposefully moved botnet C&C servers to less friendly or less advanced jurisdictions[123], thereby avoiding judicial cooperation between nations due to either unwillingness to cooperate on part of the attack source country, or the lack of a legal framework for that purpose. Specifically, unrecognised jurisdictions such as the breakaway Moldovan region of Transdniester were also referred to as having been used as the set-off location for launching attacks.[124]

119 'Riigiprokuratuur: Vene saatkond esitas valeväiteid'. Postimees, 11 July 2007 (*In Estonian*). Available at: http://www.euro.postimees.ee/120707/esileht/siseuudised/271694.php

120 'Venemaa keeldub endiselt koostööst küberrünnakute uurimisel'. ERR, 13 Dec 2008. Available at: http://uudised.err.ee/index.php?06147571

121 *Id.*

122 *Id.*

123 Kash, *supra* note 83.

124 Yasmann, *supra* note 87.

As of summer 2009, the only person convicted for participation in the cyber attacks is Dmitri Galushkevich, a 19-year-old Estonian citizen of Russian ethnicity and an IT student at Tallinn University of Technology. His role in the incidents was launching ping flood attacks (DoS attacks) against the website of the Estonian Reform Party as an expression of protest against the Government of Estonia. He was prosecuted based on Article 206 (2) of the Estonian Penal Code for illegal blocking of computer data with the purpose of hindering the functioning of the computer system.[125]

Galushkevich admitted to have, upon coordination with other, unidentified persons, used DoS (ping) attacks against the server running the public website as well as the Intranet site of the Reform Party between 25 April to 4 May. By doing this, he caused also other services run on that server to become inaccessible, thereby causing damage to the ISP and the Reform Party in the amount of ca € 2820. Both the ISP and the Reform Party dropped the claim on the condition that Galushkevich agree to a compromise procedure. Galushkevich was fined in the amount of 17 500 kroons (ca € 1120); in addition, he had to pay compensation levies[126] in the amount of 5400 kroons (ca € 345).[127]

Lessons learned for Estonia: widening the scope of criminal law

Regardless of the cyber attacks being prosecuted as "regular" cyber crime, a perception was there that the Estonian events were something "more" than simply a series of individual cyber crimes. The concertedness, intensity and wide scale, but also the nature of the targets chosen made it clear that the existing cyber crime legal framework with its perception of cyber crime as mainly conducted on the motive of material gain or mere hooliganism was too narrow in fitting these new kind of events.

125 Judgment of Harju County Court of 13 December 2007 in criminal matter No 1-07-15185 (Galushkevich)

126 Compensation levies is a payment that the convict is obliged to pay upon judgment of conviction. The size of the levies is defined based on two criteria: gravity of the crime and the applicable minimum salary. The levies is collected for state compensation for victims of crime.

127 Judgment of Harju County Court, *supra* note 125.

Due also to the complications that arose in prosecution (that were discussed in more detail above), the Ministry of Justice prepared a comprehensive amendment package to the Penal Code which was presented to the *Riigikogu* (Estonian Parliament) in December 2007 and adopted as law in February 2008.[128]

The amendments itemised in more detail the provisions of the Penal Code relating to attacks against computer systems and data, and updated the extent of some provisions (such as adding the dissemination of spyware and malware) and added a new provision on preparation of cyber crimes. Based on an understanding that the frequency of cyber attacks has been on a steady increase, and that due to the rising availability of Internet and growing use of electronic channels by the population such attacks are becoming increasingly dangerous, the amendments also prescribed higher maximum punishments for such crimes. Moreover, since collecting of evidence is complicated in investigating such crimes, the use of surveillance measures was made more easily available for the police.[129]

The composition of 'terrorist crime' in the Penal Code was amended to include 'interference with computer data or hindrance of operation of computer systems as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population'.[130] In other words, cyber crimes, if motivated by terrorist aims, are now treated as terrorist crimes by Estonian law.[131]

Similar provisions exist in some other European countries: the French *Code Penal* considers computer crimes committed intentionally with the purpose of seriously disturbing public order by frightening the population (Article 421-1, section 2) to be a terrorist crime; the Austrian *Strafgesetzbuch* considers as terrorist crime "the damaging of computer data if such action causes a threat to life or assets in great extent" (Article 278c section 1 subsection 6); the Luxembourg *Code Penal* in Article 135-1 criminalises any crime that is committed with a terrorist purpose, if at least a three-year imprisonment is foreseen for that crime.[132]

Lessons learned for Estonia: adopting the Cyber Security Strategy

The attacks accelerated an important undertaking in terms of national security: the drafting and adoption of the Estonian Cyber Security strategy. A Cyber Security Strategy Committee was formed for drafting the strategy for the period of 2008–2013, led by the Ministry of Defence in cooperation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs and the Ministry of Foreign Affairs. [133] The strategy was submitted to the Government and adopted in May 2008.

While a thorough introduction and analysis of the strategy would be beyond the scope of this paper, we would like to give a short overview of the main concepts the strategy offers, and of the action plan for its implementation.

The strategy points out the importance of understanding that the security risk posed by the asymmetric threat of cyber attacks coupled with the inherent vulnerabilities of cyberspace

128 The English translation of the Estonian Penal Code is available at the website of the Estonian Ministry of Justice at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik

129 Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code (116 SE). (*In Estonian.*) December 2007. Available at: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20090902161440&file_id=198499&file_name=KarS%20seletuskiri%20(167).doc&file_size=66048&mnsensk=166+SE&etapp=03.12.2007&fd=29.10.2008

130 Estonian Penal Code (RT I 2001, 61, 364; 2009, 39, 261), § 237

131 Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code, supra note 129.

132 As referenced in the Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code, *supra* note 129.

133 'Cyber Security Strategy'. Cyber Security Strategy Committee, Ministry of Defence. Tallinn 2008. The English version of the Estonian Cyber Security Strategy is available at: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf

is a global one, therefore solvable only by coordinated efforts of all nations. It stresses the significance of implementing organisational, technical and regulatory information security measures, but also sets a higher objective of developing a broad and sophisticated cyber security culture. Through these different layers, the Cyber Security Strategy seeks to reduce the inherent vulnerabilities of cyberspace in the nation as a whole.[134]

In order to accomplish these aims, activities are foreseen in five main policy fronts[135]:

- *The development and large-scale implementation of a system of security measures*, where every information system acknowledges the risks related to the disturbance of the service he or she provides, and has up-to-date and economically expedient security measures accessible to them and implemented. Activities are foreseen for increasing the resistance of critical information systems and infrastructure, but also at strengthening the physical and logical infrastructure of the Internet as a core platform for the majority of public services.
- *Increasing expert awareness and competence in cyber security* by developing national expertise in and high awareness of information security to the highest standard of excellence; providing high quality and accessible information security-related training, establishing common requirements for IT staff competence in information security, and by intensifying research and development in cyber security. Also, measures are proposed to ensure readiness in managing cyber security crises in both the public and private sectors.
- *Improvement of the legal framework for supporting cyber security*, including the development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems, developing legislation on protection of the critical information infrastructure, and participation in international law-making in the field of cyber security.
- *Bolstering international cooperation* by developing cooperative networks in the field of cyber security, and promoting awareness on and adoption of international treaties regulating cyber crime and cyber attacks. Beside the regulatory approach, the activities are directed at achieving a worldwide moral condemnation of cyber attacks, while recognising the need to promote and support human rights and democratic freedoms.
- *Raising public awareness on cyber security* from the grassroots (computer user) level to the widest international field.

The strategy also defines fields of Estonia's critical infrastructure.[136]

According to the strategy, the procurement of national cyber security in Estonia will be pursued by integrating cyber security action plans into the routine processes of national security planning and involving coordinated efforts of all concerned stakeholders, placing the responsibility for awareness and action on every member of the information society: not only the policymakers, law enforcement authorities and service providers, but every information system owner and finally, every computer user. [137]

Despite the high attention to security measures, the strategy stresses that the overall task rests on the need to balance, on the one hand, the risks associated with the use of information systems and, on the other hand, the indispensability of extensive and free use of information technology to the functioning of open and modern societies, wherefore appropriate attention must be paid to the protection of human rights, personal data, and identity.[138]

The practical implementation of the strategy is set out in implementation plans, which focus on the concrete actions and funds needed to achieve the objectives of the Strategy in its various fields of competence. The Implementation Plan covering years 2008–2010, elaborated based on proposals from different state agencies and working groups, was adopted in May

134 'Cyber Security Strategy', *supra* note 133. P. 3.
135 *Id.*, pp. 27-34.
136 *Id.*, p. 36.
137 *Id.* pp. 7-8.
138 *Id.* p. 6.

2009.[139] Another one will be developed for years 2011–2013. The implementation and overall efficiency of the Strategy in meeting its stated objectives will be annually assessed and reported by the Cyber Security Council of the Security Committee of the Government of the Republic.

The emerging trend of "patriot hacking"

The Estonian event was not the first occurrence of the phenomenon of "patriot hacking", but the extent and duration of the attacks to draw renewed attention to the problem. "Patriot hacking" (or "patriotic hacking")[140] is a term that reflects citizen involvement with hacking or cyber attacking the systems of a perceived adversary (e.g. another government or nation).[141]

Patriot hacking is often used as response against a country's political decision that the country where the particular hacker or group of hackers originates from openly or presumably disapproves. As such, patriot hacking is performed by a group of people who take action "pro patria" in cases where they believe that this is the right thing for their government to do or where they perceive the government as unable to do "the right thing". In the Estonian case, such expression took the form of political activists expressing their protest by engaging in coordinated cyber attacks against the online presence and, to a smaller degree, the Internet infrastructure of Estonia.[142]

The definition of "hacking" by itself is motivation-neutral – it does not differentiate whether the aim be material gain, personal revenge, curiosity or a strong political (or other social) opinion. The concept of hacking involves unauthorised access to computer data or network with the purpose of harming the integrity, confidentiality and availability of that data or network.[143]

Most regulation that relates to criminalising hacking is stemming from the understanding of an activity motivated by material gain, as it is there where most harm arises. Likewise, the Council of Europe Convention on Cybercrime[144] also seems to have mainly pecuniary consequences in mind, even though the convention can be applied to tackle hacking in a motivation-neutral way if adequately implemented. Politically motivated attacks seem to have been less in the regulatory focus, probably due to the relatively short history of widespread use of hacking as a political tool. The latter is presumably conditioned by the fact that in contrast to hacking motivated by financial gain, there is little direct reward for "political hacking" – therefore, resources are needed which assumes the involvement of organised activity at some level. Also, the technical base for hacking has in recent years become exponentially more available to regular users, who need not possess advanced technical knowledge or expensive tools to cause significant nuisance.

While patriot hacking may be perceived as more "noble" compared to other types of hacking referenced above in that it is not motivated by financial gain, and has therefore experienced more toleration, it has hazardous effects both toward its target and origin jurisdictions. Patriot hacking is understandably harmful against the target jurisdiction, as it is intended to achieve a political goal by pressuring the authorities or influencing the public. But it also has a hazardous effect towards the jurisdiction of origin in that patriotic hackers assume on their own accord a role on behalf of their governments ("taking the matter in their own hands on behalf of an

139 'Valitsus kiitis heaks küberjulgeoleku strateegia rakendusplaani aastateks 2009–2011'. Postimees, 14 May 2009 *(In Estonian)*. Available at: http://uudisvoog.postimees.ee/?DATE=20090514&ID=204872

140 The actual extent of the activity titled 'hacking' is wider than the common perception of the name indicates, since the same term is also used for actions directed at the availability of computers or computer systems (e.g. committing DoS or DDoS attacks), not only breaching into systems (i.e. the 'confidentiality' and 'integrity' aspect).

141 'An Expert Look at Chinese Information Operations Theory'. IntelliBriefs, 10 November 2008. Available at: http://intellibriefs.blogspot.com/2008/11/expert-look-at-chinese-information.html

142 RFE/RL cites Sergei Markov, a State Duma Deputy from the Unified Russia party, in his comment on the Estonia 2007 cyber attacks: "Turns out it was purely a reaction from civil society [···] and, incidentally, such things will happen more and more." *See* Coalson, Robert. 'Behind The Estonia Cyberattacks'. RFE/RL, 6 March 2009. Available at: http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html

143 *See* Bidgoli, Hossein. 'Handbook of information security', Volume 3. John Wiley and Sons, Inc, 2003. P. 560; Convention on Cybercrime (ETS No. 185), Explanatory Report. Available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm. Section 44.

144 Convention on Cybercrime, Council of Europe (ETS 185). 23.XI.2001. Available at: conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

incapable state") by going beyond condemning certain activities (which would be a legitimate exercise of freedom of expression) and instead attacking the position of another sovereign, thereby raising the question of state attribution.

The distinction lies in the understanding that a government in a similar political circumstance, if it ordered a cyber attack against another government's information services, would be exposed to state liability, whereas "private hacking initiatives" would be regarded as "ordinary" cyber crime. A convenience for political hackers is that their motivation is covered by the political situation between two governments and therefore will not need to be expressed as part of their identity (which would normally be the case with terrorist groups). This combination leaves patriotic hackers in a gray area of law where their activities may be significantly more disturbing than those of "ordinary hackers", but the legal framework for investigation and prosecution does not recognise any difference.

Regardless of motivation, hacking and cyber attacking cause harm also to communications network infrastructure, including the global Internet infrastructure, in that they overload the normal capacities of networks. Where botnets are used to carry out politically motivated attacks – like the Estonian (and later on also Georgian) examples indicate – the low risk of facing prosecution due to attacks being "only political" feeds the "business incentive" of botnet owners to continue producing and distributing malicious software.

Therefore, there is not much basis for tolerating patriot hacking as "less harmful" or as a semi-legitimate expression of protest. There are legal ways for citizens to express their opinion and attitude without effectively hampering information society in another country. Communications undertakings and infrastructure owners have a legitimate expectation that the state endeavours to provide a secure environment for their business activities. This is also in end user interests, who individually have little chance to defend themselves against the service disruptions caused by cyber attacks. In order to support the functioning and development of information society, the focus of both national and international criminal law needs to widen to take the full spectrum of threat into account. Additionally, widening the scope of national criminal law to include politically motivated cyber attacks in the definition of cyber crime would send a clear message that the government does not condone patriot hacking on its behalf, thereby relieving the risk of government facing international allegations of state involvement in the event that its nationals or residents should engage in such activities.

The Estonian incident offered lessons to be learned for both the target and the originating side; the Georgian incident occurring about a year later demonstrates that lack of a negative reaction from the state encouraged attackers to return to their tools in a more concerted manner when a suitable opportunity arose. To apply the old proverb "Wise men learn from their mistakes, but really wise men learn the mistakes of others": the sooner a general consensus develops regarding the dangerous nature of politically motivated cyber attacks, and the sooner the appropriate legislative steps are taken, the better protected information societies in individual nations, but also information society as a global good will be.

IV Summary of the Estonian case

INCIDENT TIME FRAME

Start Friday, 27 April 27 2007

End Friday, 18 May 2007 (some aftermath until end of May 2007)

Duration 3 weeks

INCIDENT CONTEXT

Political context and background of incident

- Government decision to relocate a Soviet-era WWII memorial from a central location in the capital city to a military cemetery met by intense opposition from the Russian government and media;
- Protests against the start of removal works break into street riots;
- Siege of the Estonian embassy in Moscow conducted by *Nashi*, a Russian political youth movement. Ambassador physically harassed.

Information society indicators

- Pioneer since mid-1990ies in state-wide public e-solutions employed by both the private and public sectors (prevalent use of Internet banking; mobile parking and public transportation tickets; online voting in elections since 2005; majority or taxes declared electronically; online State Portal as a one-stop service point for all government e-services)
- Internet access nearly universally available (98% of territory), mobile penetration nearing 100% (in 2007);
- Overarching governance policy, backed by a legal framework, to use information technology to increase public sector administrative capacity and ease citizen-to-government communications. Paperless government since 2001.

INCIDENT FACTS

Methods

- DoS and DDoS;
- Website defacement;
- Attacking DNS servers;
- Mass e-mail and comment spam.

Targets

- Servers of institutions responsible for the Estonian Internet infrastructure;
- Governmental and political targets (parliament, president, ministries, state agencies, political parties);
- Services provided by the private sector (e-banking, news organisations);
- Personal and random targets.

Origin

- Mainly sourced outside of Estonia, computers involved from 178 countries altogether;
- Early attacks largely carried out by nationalistically/politically motivated individuals and following instructions provided on Russian-language Internet forums and websites;
- The second phase of attacks has features of central command and control;
- A few self-proclaimed or self-acknowledged attackers;
- Russian authorities have denied any involvement.

Effect

- Perceptible effect to the functioning of domestic economy: affecting sectors of commerce, industry and governance that rely on ICT infrastructure and electronic communications in their daily conduct of business (banks, media corporations, governmental institutions, small and medium size enterprises);
- Societal effect: hindered access to communication with public administration (unavailability of information, means of communication, and access to services);
- Information flow to the outside world im-

paired;

- Side-effects: attack mitigation means blocked off part of the genuine traffic together with the malicious one.

Measures taken

- Response coordinated by CERT-EE, with assistance from system administrators and experts both within and outside of the country; IT experts from both public and private sectors engaged round-the-clock;
- Technical measures: increasing bandwidth, using multiple servers and/or connections; firewalling, filtering out malicious traffic; application of security patches; use of attack detection systems, etc. Some sites temporarily switched to "lightweight mode";
- International cooperation, organised by Ministry of Defence: informing partners in EU and NATO; observer and advisory assistance from NATO network incident handling entities; national CERTs (e.g. U.S.A., Germany, Finland) assisted in locating and reporting sources of attack;
- Public awareness: news about Estonia cooperating with foreign authorities to locate cyber criminals and bring them to justice reduced the number of spontaneous attackers.

LEGAL LESSONS IDENTIFIED AND LEARNED

Core of the case

- Highlighted the need to raise international awareness about crimes against information society;
- Raised the question of efficiency of mutual criminal assistance treaties in a situation where the receiving party is unwilling to cooperate.

Summary

- The traditional view of substantive criminal law considers cyber crime foremost as an economically motivated activity, which may not be sufficient to satisfactorily respond to politically motivated cyber attacks where the damaged legal interest is not the integrity, availability, confidentiality or the proper functioning and use of computer data, programs, or networks, but the political, constitutional, economic or social structure of the state;
- There are often differing legal requirements for what is permissible in criminal proceedings in the countries involved; and the attackers may resort their activities to jurisdictions that the attacked country – or the country receiving a request for assistance – does not recognise, which will foreclose the success of criminal proceedings. International law lacks effective enforcement mechanisms to ensure cooperation from the country in which the attacks originate, if the latter in refuses to cooperate. But international cooperation in criminal matters, in its mainly bilateral nature, may be ineffective even if both parties are willing and able to cooperate, as the Internet facilitates easy splitting up of a given illegal act to several small trails that can be left in a number of countries – such as the formation of a botnet to attack servers in a particular country.

Challenges

- Reorientation from a "whose area of responsibility a particular type of cyber attack might be" to an understanding that a national-scale cyber attack is a problem affecting the society, its security and public order as a whole, and therefore the legal framework needs to specify at what degrees of cyber attacks the different institutions are entitled to and obliged to interfere, and what are the procedural rules and the relevant institutions' terms of reference in case of wide-scale cyber incidents.
- A lack of unison of regulation between countries leads to a fragmented approach toward a phenomenon that knows no borders; a wider platform of multilateral cooperation is therefore needed to handle such threats. Also, the development of international agreements and uniform standards of best practice by the relevant international players would be highly welcome, specifying the organisational framework, terms of reference, and procedural rules applicable in the event of a cyber attack.

INCIDENT TIMELINES

Estonia 2007

Friday, 27 April

- Simultaneous attacks against multiple websites of the Estonian government and government agencies.
- Access to websites temporarily limited for users located outside of Estonia.

Saturday, 28 April

- Multiple-sourced DDoS attacks.

Sunday, 29 April

- Malicious attacks originating from outside of Estonia.
- Access for users situated outside of Estonia limited due to technical countermeasures taken to handle the attacks.

Monday, 30 April

- Cyber attacks continue.
- Attempts to halt the functioning of the entire public sector data communications network.

Tuesday, 1 May

- Increased attacks against the Estonian cyber space in the early hours of the morning. The volume of attacks has gradually increased, but the situation remains under control.
- Attacks mainly targeted against the web and name servers of government entities.
- Short breaks in the availability of websites within Estonia, but these were caused by implementing new technical countermeasures.
- Three serious attacks against web traffic at 8 PM, midnight, and 1 AM, after which the situation normalised.

Wednesday, 2 May

- Communications networks operate normally, and websites of the Estonian government agencies (or at least their minimised versions) were viewable both in- and outside of Estonia.

Thursday, 3 May

- Volume of Internet traffic still above the normal range.
- Data communications networks were kept up by implementing security measures and adding extra server capacity.
- In addition to government entities, attacks against online media outlets and private enterprises.
- A large DDoS attack against government Internet traffic and web servers, which was put off in cooperation between Internet Service Providers.

Friday, 4 May

- Reports of increased volumes of spam-email.
- In early morning, the availability of Estonian websites unstable for users located abroad.

Saturday, 5 May

- The situation is relatively calm.

Sunday, 6 May

- The situation is relatively calm.

Monday, 7 May

- International cooperation in fending off the attacks is starting to clearly pay off.
- In order to minimise possible risks, all government and private sector IT specialists, as well as home users, were requested to pay special attention to security settings of their computers and networks in order to avoid being taken under hacker control.

Tuesday, 8 May

- At 11 PM, a large cyber attack commenced that carried on for a long time.
- The primary targets were still government websites and data communications networks.

Wednesday, 9 May

- Cyber attacks appear to be attempting a "cyber blockade" of Estonia.
- Dissemination of information hindered from Estonia to the outside world.

Thursday, 10 May

- Continued cyber attacks attempting a cyber blockade.
- Many parallel large-volume attacks that lasted

a long time.

- Both the public and the private sector targeted.
- The work of Hansabank (the country's largest bank) Internet channels disturbed.

Saturday, 12 May to Sunday, 13 May

- No major attacks reported.

Monday, 14 May

- Minister of Defence raises the issue of cyber attacks against Estonia at a meeting with EU defence ministers.

Tuesday, 15 May

- Attacks against the second largest commercial bank, SEB Eesti Ühispank.

Wednesday, 16 May

- By midnight, single large attacks had subsided to weekend level.

Friday, 18 May

- Continued filtering of network traffic in cooperation among IT security staff of public and private sector entities in coordination with CERT-EE.

Source of data: State Informatics Centre

Radio Free Europe/ Radio Liberty 2008

Saturday, 26 April

- The website of RFE/RL Belarus service hit by a DDoS attack at 8 AM.
- In a few hours, DDoS attacks expand against seven other RFE/RL websites: RFE/RL in Kosovo, Azerbaijan, Tatar-Bashkir, South Slavic, Tajik, and Radio Farda.

Saturday, 27 April

- Attacks continue.

Monday, April 28

- Most of the RFE/RL Internet sites restored.
- Radio Svaboda back online in the evening.

Lithuania 2008

Saturday, 28 June

- Cyber attacks commence against Lithuanian websites.

Sunday, 29 June

- Attacks peak at 5 to 6 PM.
- 300 internet sites defaced at the peak of the attacks.

Monday, 30 June

- Attacks still ongoing.

Tuesday, 1 July

- Most sites restored to original content.

Georgia 2008

Saturday, 19 July to Sunday, July 20

- The website of Georgian President Mikheil Saakashvili becomes unavailable for more than 24 hours due to a multi-pronged DDoS attack. The website temporarily moves to US server.

Friday, 8 August (7 August according to some sources)

- DDoS attacks begin against Georgian government sites.
- Coordinated cyber attacks against Georgia's Internet infrastructure. Several Georgian state computer servers come under external control.
- The Georgian government switches to hosting locations to the USA; the Ministry of Foreign Affairs opens a Blogspot account to disseminate information.
- Multiple C&C servers attacking websites that are Georgian or sympathetic to the country.
- Prolonged attacks against the websites of the Georgian President, the central government, the Ministry of Foreign Affairs and Ministry of Defence. The latter three remain unavailable at least until 11 August.
- Some commercial websites taken over.