CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

Cyber Attacks Against Georgia: Legal Lessons Identified

Eneken Tikk, Kadri Kaska, Kristel Rünnimeri,
Mari Kert, Anna-Maria Talihärm, Liis Vihul

NATO Unclassified
Version 1.0
November 2008

DISCLAIMER

This analysis document is a product of the CCD COE Legal Task Team[1].

It is intended for educational purposes to promote public discussion and to keep readers informed on topics of common interest.

The views, opinions, and/or findings and recommendations contained in this analysis are those of the authors and should not be construed as an official position, policy, or decision of NATO or its agencies.

Point of Contact – Ms Eneken Tikk - eneken.tikk@mil.ee

[1] The CCD COE Legal Task Team is a project team formed by the Director of COE on the basis of the CCD COE Operation MOU, with the function of optimising implementation of the legal projects of the COE and providing legal assistance to other projects and branches of the COE.

Georgian Cyber Attacks: Legal Lessons Identified

Contents

I INTRODUCTORY REMARKS 3

II FACTS OF THE CASE 4

Background and Context of Cyber Attacks against Georgia 4
Georgia as an Information Society 5
Methods of Cyber Attacks 7
Defacement of Websites 7
DoS and DDoS Attacks 8
Distribution of Instructions and Malicious Software 9
Other Types of Attack 10
Origin of the Attacks 12
Countermeasures 14
Effects of the Attacks 15

III LEGAL LESSONS IDENTIFIED FROM THE GEORGIAN CASE 18

The Applicable Legal Regime 18
Applicability of International Humanitarian Law 18
Rationale of questioning the applicability of LOAC 18
General prerequisites for the applicability of LOAC 19
Applicability of National and International Criminal Law 23
Rationale of questioning the applicability of criminal law 23
Georgian Criminal Law in the Field 24
Applicability of ICT Legal Framework 25

IV CONCLUSIONS 29

ANNEX I: FACTS ABOUT SOUTH OSSETIA 32

ANNEX II: ATTACKS ILLUSTRATED 34

ANNEX III: CHRONOLOGY OF CYBER ATTACKS AGAINST GEORGIA 36

ANNEX IV: ESTONIAN INFORMATION SOCIETY IN FACTS 42

ANNEX V: GEORGIAN INFORMATION SOCIETY IN FACTS 43

ANNEX VI: COMPARISON OF RECENT CYBER CONFLICTS 44

I Introductory Remarks

Aim of the analysis. The purpose of this paper is to present a balanced and inclusive outline of the facts about cyber attacks[2] against Georgia that took place in August 2008, and to indicate the legal implications of those incidents. In addition, this paper aspires to compare these facts to the legal lessons identified from the Estonian case[3] in order to discern emerging trends of cyber incidents and to identify their implications to the current legal framework.

Sources of information. The facts of the Georgian cyber attacks have been collected from the Estonian Computer Emergency Response Team (CERT-EE) and distinguished IT security websites[4], verified with the Georgian Embassy in Estonia, and compared with international media[5]. The majority of the materials referred to in the facts section and all materials referred to in the analysis part are open-source.

Target audience: Policymakers and researchers involved in the development of national or international cyber security and cyber defence-related concepts and initiatives; IT experts engaged in defensive measures against similar type of incidents; wider public interested in recent developments in national cyber threat issues.

---

[2] The term 'cyber attack' is used throughout this paper as the term that has gained wide public use by both media and the IT society. The term 'attack' is not to be confused with the term 'armed attack' within the meaning of international humanitarian law, the relevance of which is discussed in more detail in Chapter III of this paper.

[3] CCD COE Legal Task Team. 'Case Study Estonia: Legal Lessons Learned from the April-May 2007 Cyber Attacks against Estonia' (draft). October 2008

[4] Dr Jose Nazario, Arbor Networks; Steven Adair, Shadowserver Foundation; Gadi Evron, Beyond Security, ZDNet, Circle ID; Dancho Danchev, Renesys; Jeff Carr, IntelFusion/Project Grey Goose.

[5] Reuters, *et al*.

II Facts of the Case

Background and Context of Cyber Attacks against Georgia

The conflict subject to the analysis falls within the timeframe and context of the broader armed conflict that broke out in August 2008 between the Russian Federation and Georgia over South Ossetia[6], an autonomous and *de jure* demilitarized Georgian region on the border of Georgia and Russia.

South Ossetia became *de facto* independent from Georgia during the 1991 Georgian-Ossetian conflict; however, it remained commonly recognised by the international community as an integral part of Georgia.[7] Despite a declared ceasefire and numerous peace efforts, the conflict has remained unresolved.

To maintain stability in the region after the 1991 conflict, a peacekeeping force was formed in 1992 under an OSCE mandate of Russian, Georgian and South Ossetia's troops. The peacekeepers were subjected to the authority of a Russian commander. In practice, these troops failed to cooperate, and tensions have gradually grown between Georgia on one side and mostly Russian-supported separatists on the other.[8]

On August 7, 2008, following separatist provocations, Georgian forces launched a surprise attack against the separatist forces.[9] On August 8, Russia responded to Georgia's act by military operations into Georgian territory, which the Georgian authorities viewed as Russia's military aggression against Georgia.[10] By late August 7, before the Russian invasion into Georgia commenced, cyber attacks were already being launched against a large number of Georgian governmental websites[11], making it among

---

[6] See *Annex I* for a outline of information regarding the status of South Ossetia and the roots of the conflict.

[7] The Russian Federation recognised South Ossetia's independence on 26th August, 2008; the Russian example was followed by Nicaragua a week later. *See* Statement by President of Russia Dmitry Medvedev on August 26, 2008. Available at: kremlin.ru/eng/speeches/2008/08/26/1543_type82912_205752.shtml (last accessed 12 Nov 2008); Nicaragua recognizes South Ossetia, Abkhazia. *Reuters*. 3 Sep 2008. Available at: www.reuters.com/article/gc07/idUSN0330438620080903 (last accessed 12 Nov 2008)

[8] Liik, K. 'Tee sõtta'. (*In Estonian)* International Centre for Defence Studies. 11 Aug 2008. Available at www.icds.ee/index.php?id=73&type=98&L=0&tx_ttnews[tt_news]=262&tx_ttnews[backPid]=214&cHash=4de7396400 (last accessed 25 Nov 2008). *See* also Council of Europe Parliamentary Assembly Resolution 1633 (2008) on 'The consequences of the war between Georgia and the Russian Federation', available at assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta08/ERES1633.htm (last accessed 20 Nov 2008)

[9] Liik, K. *Id*.

[10] *Georgian Ministry of Foreign Affairs*. Information for Press. 8 Aug 2008. Available at: www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=461&info_id=7193&date=2008-08-08&new_month=08&new_year=2008 (last accessed 14 Nov 2008)

[11] 'Georgia, Russia: The Cyberwarfare Angle', *Stratfor Today*, Aug 12, 2008, available at: www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle (last accessed: 18 Nov 2008).

the first cases in which an international political and military conflict was accompanied – or even preceded – by a coordinated cyber offensive. [12, 13]

On the August 8, the President of Georgia, Mikheil Saakashvili, informed the international community of having begun mobilisation, and on August 9, 2008, Georgia imposed a "state of war"[14,15]. Even though this step foremost served as a national measure in a situation where Georgia perceived a threat to national security and sovereignty, this also set the framework applicable as Georgia dealt with the cyber attacks and as such, is relevant to keep in mind when studying Georgia's response to the cyber attacks.

Georgia as an Information Society

Statistics about the Georgian ICT sector show that Georgia has 7 Internet users per 100 people (*e.g.* Estonia, the country that fell under similar type of attacks in 2007, has 57, and Lithuania who came under coordinated cyber attacks in summer 2008[16], has 32).[17] The relatively low number of Internet users in Georgia reflects the nation's infrastructural capacity and its lack of overall dependence on IT-based infrastructure. However, the number of Internet users has been steadily growing – the Georgian National Communications Commission (the Georgian regulatory authority in the

[12] Although intense cyber attacks started taking place as the political conflict between Georgia and Russia escalated, Georgia had also experienced cyber incidents prior to the land invasion: from July 19 to 20, 2008, the website of the President of Georgia came under a persistent DDoS attack. *See*, e.g, Adair, S. 'Georgian Attacks: Remember Estonia?', *Shadowserver Foundation*, Aug 13 2008, available at: www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080813 (last accessed: 14 Aug 2008).

[13] The roots of using cyberspace as an extension to the conflict on the ground date back into the first Chechen war in 1994, when the Chechen separatist movement was using Internet as a tool for delivering powerful pro-Chechen and anti-Russian propaganda. During the second Chechen war in 1999-2000, Russian officials were accused of hacking into Chechen websites and thus escalating the cyber conflict. Cyber attacks were also conducted simultaneously to the Kosovo war in 1999, when NATO Internet infrastructure and U.S. and U.K computers became under attacks. Also, a DDoS attack was conducted allegedly by pro-American hackers against *Al Jazeera* (an Arabic news channel) website during the last Iraqi war. Since 2000, every now and then, as political tensions have risen between the parties of the Middle East conflict, Israeli and Arab combatants have used cyberspace in order to pursue their political aims. *See, e.g.*, Kenneth Geers, 'Cyberspace and the Changing Nature of Warfare', *Cooperative Cyber Defence Centre of Excellence*, 2008; see also Bruce Schneier 'Cyberwar in Estonia', 23 Aug 2007, available at: www.schneier.com/blog/arch (last accessed 25 Nov 2008)

[14] Press release of the President of Georgia. Declaration of Universal Mobilization by Georgian President Mikheil Saakashvili. Aug 8, 2008, available at: www.president.gov.ge/?l=E&m=0&sm=1&st=0&id=2689 (last accessed: 25 Nov 2008)

[15] [Elise Labott, E., Gotsadze, E.] Russian warplanes target Georgia. *CNN*, August 9, 2008. Available at: edition.cnn.com/2008/WORLD/europe/08/09/georgia.ossetia/index.html?eref=rss_topstories (last accessed 25 Nov 2008). According to Georgian officials referenced in the article, the order was not a formal declaration of war and stops short of declaring martial law; it did give the President powers that he would not have had in a peacetime situation, such as issuing curfews, restricting the movement of people or limiting commercial activities.

By a decision of the Georgian Parliament, the state of war was lifted on September 3, 2008.

[16] CCD COE Legal Task Team case study regarding the July 2008 cyber attacks against Lithuanian websites. Draft as of November 2008.

[17] Internet users per 100 population, 2006. Available at: data.un.org/Data.aspx?d=MDG&f=seriesRowID:605 (last accessed: 25 Nov 2008)

electronic communications sector) reported an 81% increase in the number of Internet users in Georgia in 2006; much of that growth is based on the growing number of broadband Internet users.[18]

Sources are varying on Georgia's interconnection dependency on Russia. Considering the geography of the region, Georgia has few options for Internet connectivity via land routes, namely Turkey, Armenia, Azerbaijan, and Russia. According to some sources, most of Georgia is, in terms of Internet infrastructure, dependent on Russia - more of Georgia's connections to the Internet pass through Russia than any other country, comprising nearly half of Georgia's thirteen links to the worldwide network.[19] On the other hand, there is strong indication also as regards interconnection with Turkey: according to Renesys, most of Georgia's 309 Internet prefixes get routed via Turkish or Azerbaijan service providers; however, the latter is then routed on via Russia.[20] As is apparent, options for dispersing data traffic are relatively limited for Georgia, which makes it a good target for coordinated cyber assault and isolation. In the Estonian cyber attacks in April-May 2007, this concern was not nearly as acute, as there are (and were at the time the attacks took place) a number of outbound high-capacity fibre optic data links to several countries (Finland, Sweden, Latvia, Russia), owned by several e-communications network operators; in addition, there were also binding agreements in effect between larger e-communications infrastructure-owning operators, enabling to divert excessive traffic to a particular ISP.[21]

As for perspectives for Georgia, building a direct high-capacity link from Georgia to Western Europe is in progress: a fibre optic cable through the Black Sea (from the coastal city of Poti, Georgia to Varna, Bulgaria) was nearly completely installed by the time the August 2008 Russian-Georgian conflict commenced.[22] When set up, this connection can be expected to remarkably enhance the country's Internet interconnectivity. It was anticipated that the system would be delivered in the autumn of 2008[23]; there is currently no open-source information available as to the status of this project after the conflict in August.

As of 2007, there are five companies operating in the Georgian Internet access and services market; of them, Caucasus Network Tbilisi, the main commercial service

---

[18] Georgia: Electronic Communications Market Turn Over Exceeds GEL 1 bln. Caucas Euronews, 08/06/2007. Available at:

www.caucaz.com/home_eng/depeches.php?idp=1723&PHPSESSID=d7e84d535388fb83449271520 99c6967 (last accessed 25 Nov 2008)

[19] 'Georgia, Russia: The Cyberwarfare Angle', *Stratfor Today*, Aug 12, 2008, available at: www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle (last accessed: 27 Aug 2008).

[20] The relevant ISPs are TTnet (AS 9121; Turkey), Delta Telecom (AS 29049; Azerbaijan), and TransTelCom (AS 20485; , Russia) *See* Zmijewski, E. 'Georgia Clings to the 'Net', *Renesysblog*, Aug 11, 2008, available at: www.renesys.com/blog/2008/08/georgia_clings_to_the_net.shtml (last accessed: 27 Aug 2008).

[21] CCD COE Legal Task Team, *supra* note 3.

[22] Zmijewski, *supra* note 20

[23] 'Tyco to construct undersea fibre-optic system for Caucasus.' *Invest In Georgia Investment Agency*. Available at: www.investingeorgia.org/news/view/274 (last accessed 14 Nov 2008)

provider, holds 90% of the market.[24] United Telecom of Georgia, the incumbent operator in the fixed line access market, also provides access to Internet service.[25,26]

More details about Georgia's information society are presented in Annex IV. For comparison, the same characteristics have been indicated for Estonia in Annex V.

Methods of Cyber Attacks

The methods of cyber attacks against Georgia primarily included defacement[27] of public websites and launch of Distributed Denial of Service (DDoS)[28] attacks against numerous targets – methods similar to those used in attacks against Estonia in 2007. A chronological overview of the attacks can be found in Annex III to this paper.

Defacement of Websites

Defacements were directed at political/governmental and financial sites, including:

www.president.gov.ge	website of Mikheil Saakashvili, the President of the Republic of Georgia
www.nbg.gov.ge	website of the National Bank of the Republic of Georgia
www.mfa.gov.ge	website of the Ministry of Foreign Affairs of the Republic of Georgia

According to data available, the website of President of Georgia, as well as the Georgian Ministry of Foreign Affairs were defaced and replaced with a collage of photos of Mikheil Saakashvili and Adolf Hitler.[29] The website of the National Bank of Georgia was reported to have been "defaced and replaced with a gallery of 20th century dictators", President

[24] Georgia: Electronic Communications Market Turn Over Exceeds GEL 1 bln. 8 Jun 2007. Available at: www.caucaz.com/home_eng/depeches.php?idp=1723&PHPSESSID=d7e84d535388fb83449271520 99c6967 (last accessed 18 Nov 2008)

[25] Hardabkhadze, V., Kvernadze, L. Georgia. (Part of a report produced for the European Commission on the electronic communications markets in Central and Eastern Europe) Available at: ec.europa.eu/information_society/activities/internationalrel/docs/pi_study_rus_ukr_arm_azerb_bel_geor_kaz_mold/7_georgia.pdf (last accessed 20 Nov 2008). p. 8

[26] CERT-EE Report on status in Georgia, August 14, 2008. A public version of the report is available at the website of the Estonian Informatics Centre at www.ria.ee/index.php?lang=en (last accessed 25 Nov 2008)

[27] A *website defacement* is an attack on a website that changes the visual appearance of the site.

[28] *DDoS* (Distributed Denial of Service) attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Methods for this vary: a DDoS attack can be carried out by means of a Trojan or other kind of malware, or via a botnet.

[29] See *e.g.* Dancho Danchev "Coordinated Russia vs Georgia cyber attack in progress," Aug 11, 2008, available at: blogs.zdnet.com/security/?p=1670 (last accessed: 18 Nov 2008); *see also* На сайте МИД Грузии появился коллаж с Гитлером' (in Russian), *Lenta.Ru*, available at: www.lenta.ru/news/2008/08/09/defaced/ (last accessed: 17 Nov 2008).

Saakashvili among them.[30] The only depiction of defacement that has been presented is a collage of photos of Mikheil Saakashvili and Adolf Hitler; thus, it is not clear at this point to the authors of this paper whether all three websites were defaced in the same way or whether two different types of defacements were carried out.

CERT-EE reported of web sites of several Azerbaijan newspapers and media agencies having been defaced (www.day.az, www.today.az, www.ans.az)[31].

DoS and DDoS Attacks

According to the information received from CERT-EE and confirmed by the Georgian Embassy in Tallinn, the Georgian websites attacked included examples from both public and private sector.

Government sites:

www.abkhazia.gov.ge	official website of the government of the Autonomous Republic of Abkhazia
www.mes.gov.ge	Ministry of Education and Science of the Republic of Georgia
www.naec.gov.ge	governmental website providing standardised educational tests for students
www.parliament.ge	the Parliament of the Republic of Georgia
www.president.gov.ge	the President of the Republic of Georgia

News and media sites:

www.forum.ge	biggest forum in Georgia
www.civil.ge	largest Georgian news page in English
www.presa.ge	Association Press
www.apsny.ge	a news portal
www.rustavi2.com	a private television company
www.news.ge	a news portal in English
interpress.ge	a news portal

Financial institutions:

www.tbc.ge	Georgia's largest commercial bank

Other websites:

[30] John Markoff quoting Gadi Evron, a well-known network security expert. *See* John Markoff "Before the gunfire, cyberattacks," International Herald Tribune, Aug 13, 2008, available at: www.iht.com/articles/2008/08/13/technology/13cyber.php. (last accessed: 17 Nov 2008).

[31] CERT-EE, *supra* note 26

www.tbilisiweb.info	News portal
www.newsgeorgia.ru	News portal
www.os-inform.com	privately owned media site
www.kasparov.ru	Web page of Russian opposition party representative
www.hacking.ge	Georgian hackers' community website
www.skandaly.ru [32]	Russian news portal

Attack statistics provided by Arbor Networks show high intensity attacks with data traffic reaching 211.66 Mbps on average and 814.33 Mbps at the maximum. Regarding duration, an average attack has lasted 2 hours 15 minutes, while the longest one lasted 6 hours.[33]

There seems to be a rather widespread consensus on that the attacks appeared coordinated since their commencement.[34] In this regard, the cyber events in Georgia differ slightly from the incidents in Estonia, where coordination was recognized only in the second phase of the cyber attacks.[35] The issue of coordination is discussed in more detail under subsection 'Origins of the attacks' of this paper.

Distribution of Instructions and Malicious Software

Several Russian blogs, forums, and websites spread a Microsoft Windows batch script that was designed to attack Georgian websites. [36] According to Steven Adair of Shadowserver, this script was posted on several websites and was also hosted on one site as a compressed downloadable file which contained an executable "war.bat" file within it.[37] The same method was used in the emotional phase of cyber attacks against Estonia, where a downloadable script to ping flood Estonian websites (both DNS and IPs) was shared on various Russian language message boards.[38]

Instructions on how to ping flood Georgian government web sites were also distributed on Russian language websites and message boards, as well as lists of Georgian sites

---

[32] One will notice that not all of these are Georgian websites. However, it is interesting to see that the same groups involved with targeting various Russian media outlets have also been taking aim at various Georgian websites. Additionally, the website of Garry Kasparov has once again come under attack. *See* Adair, S. 'Georgian Websites Under Attack - DDoS and Defacement', *Shadowserver Foundation,* Aug 11, 2008, available at: www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080811 (last accessed: 27 Aug 2008)

[33] Nazario, J., 'Georgia DDoS Attacks - A Quick Summary of Observations', *Arbor Networks*, Aug 12, 2008, available at: asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/> (last accessed: 14 Aug 2008).

[34] *See* Danchev, *supra* note 29; 'Georgia, Russia: The Cyberwarfare Angle', *Stratfor Today*, Aug 13, 2008, available at: www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle (last accessed: 21 Aug 2008).

[35] CCD COE Legal Task Team, *supra* note 3.

[36] Adair, S. "Georgian Attacks: Remember Estonia?", *Shadowserver Foundation*, Aug 13, 2008, available at: http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080813 (last accessed: 25 Nov 2008).

[37] *Id.* A redacted version of the script can be accessed at www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080813 (last accessed 18 Nov 2008)

[38] CCD COE Legal Task Team, *supra* note 3. Note that instructions for cyber attacking Estonian sites continue to be available on the Internet even at the time of this analysis.

vulnerable to remote SQL injections, facilitating automatic defacement of them.[39] Again, this was similar to the Estonian case, where instructions on carrying out cyber attacks were spread almost exclusively on Russian language sites, regardless of whether those sites were located in Estonia, Russian Federation, or elsewhere. It is relevant to mention that in both Georgia and Estonia, Russian is a minority language, and in neither of those two is it an official language.[40]

According to the analysis of the Swedish National Defence University[41], and supporting conclusions by Shadowserver, stopgeorgia.ru (also utilizing 'stopgeorgia.info' as a redirect) provided DDoS attack tools for download and indicated a number of .ge web sites as a priority for attack. The findings of an analysis by the Project Grey Goose[42] confirm evidence of co-ordinated targeting and attacking of Georgian websites, and point out that the same sites (stopgeorgia.ru/stopgeorgia.info) also provided the necessary attack tools for the cyber assault against Georgia for hackers.[43] In summary, 36 major web sites were identified as targets for hackers, among those the Embassies of the US and UK in Tbilisi, the Parliament, Supreme Court, and Ministry of Foreign Affairs of Georgia, several news and media resources, and numerous other sites. [44]

Other Types of Attack

There were also signs of abuse of public lists of e-mail addresses of Georgian politicians for spamming and targeted attacks. The list of e-mail addresses was originally created by a lobbying organisation; during the attacks, it was circulated "in an attempt to convince Russian hackers of the potential for abusing it in spamming attacks and targeted attacks presumably serving malware through live exploit URLs". [45]

---

[39] Danchev, *supra* note 29.

[40] In Georgia, two of the major languages spoken include language Georgian (71%) and Russian (9%); in Estonia, Estonian is the first language for 67.3% and Russian for 29.7% of the population.

See Georgia. *CIA World Factbook* (Updated as of 6 November 2008). Available at: www.cia.gov/library/publications/the-world-factbook/geos/gg.html (Last accessed: 17 Nov 2008)

Estonia. *CIA World Factbook* (Updated as of 6 November 2008). Available at:

www.cia.gov/library/publications/the-world-factbook/geos/en.html (Last accessed: 17 Nov 2008)

[41] E-mail from the Swedish Defence University with preliminary conclusions on 'Cyberattack against Georgia'. August 2008

[42] Project Grey Goose was a volunteer effort of IT experts, led by Jeff Carr of IntelFusion in cooperation with Palantir Technologies, to understand the nature of recent cyber activities between Russia and Georgia. The Project undertook an in-depth OSINT research into the communications regarding cyber attacks spread over Russian hacker sites in August 2008; a report on the findings is available at www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report

[43] Project Grey Goose. Phase I Report Russia/Georgia Cyber War – Findings and Analysis. 17 October 2008. www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report (last accessed 31 Oct 2008)

[44] *See* a list of target sites in Annex II of this paper.

[45] Danchev, *supra* note 29.

The same method was used against Estonia, where comment and e-mail spam comprised a remarkable load on both private and governmental web and e-mail servers.[46] Considering that the law governing administrative procedure in Estonia ensures the right of every person to conduct operations with the state via electronic means[47], crippling the habitual communication channels not only constituted an inconvenience but also harmed the state's ability to carry out its administrative functions in accordance with applicable law.[48]

There is a reference to attempts to conduct a "cyber blockade" on Georgia by directing all Georgian Internet traffic through Russia, but the reliability of the source reporting this is not verified.[49] Apparently, trace route searches for the websites of the Georgian Ministry of Foreign Affairs (mfa.gov.ge), Georgian Ministry of Defence (mod.gov.ge), and the website of the Georgian President (president.gov.ge) were showing blocked access via TTNet (Turkey) upon inquiries from both the USA and Ukraine.[50] Still, a similar detail was also reported by Dancho Danchev (ZDNet), who noted that cyber attacks expanded to Turkey and the Ukraine, where many of the servers which route traffic to Georgia were commandeered, possibly by the Russian Business Network (RBN)[51].[52]

---

[46] CCD COE Legal Task Team, *supra* note 3.

[47] Administrative Procedure Act, RT (Estonian State Gazette) I 2001, 58, 354; 2007, 24, 127. An English translation is available at 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 (last accessed 18 Nov 2008); *see* Articles 5(6), 25(1).

[48] The DDoS attacks on the government websites and portals during the April-May 2008 cyber attacks in Estonia had a similar effect. According to art 32 of the Estonian Public Information Act (RT I 2000, 92, 597; 2007, 68, 420; English text available at www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40095K2&keel=en&pg=1&ptyyp=RT&tyyp=X&query=avaliku+teabe), state and local government agencies are mandated to publish certain information on their websites that is not published elsewhere. Also, numerous public registries only operate online.

[49] Russian Invasion of Georgia/Russian Cyberwar on Georgia. 9 October, 2008. The report is accessible at www.georgiaupdate.gov.ge. It must be noted that the report is anonymous and hosted by Georgia-friendly actors. The conclusions of this report have thus not been relied on in this analysis. It provides a good overview of foreign media review on Georgian cyber events in an annex.

[50] *Id.*

[51] Russian Business Network. A cybercrime organisation, specialising in phishing, malicious code, botnet command-and-control (C&C), denial of service (DoS) attacks, and identity theft. Further information is available at: www.verisign.com/security-intelligence-service/info-center/webcasts/archived/index.html (last accessed: 27 Aug 2008); B. Krebs, "Shadowy Russian Firm Seen as Conduit for Cybercrime", *Washington Post*, Oct 13, 2007, available at: www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html (last accessed: 27 Aug 2008).

[52] E. Zuckerman, 'Cyber Attacks: Misunderstanding Cyberwar in Georgia', *Postchronicle,* Aug 17, 2008, available at: www.postchronicle.com/news/technology/article_212165469.shtml (last accessed: 27 Aug 2008). *See* also E. Zuckerman, 'Misunderstanding Cyberwar', Aug 18, 2008, available at: www.worldchanging.com/archives/008381.html (last accessed: 27 Aug 2008).

See *supra* note 51 for references regarding RBN.

Danchev reports of an example of attempts to isolate the Georgian Internet user community and prevent their communication via usual channels: one of Georgia's most popular hacking forums was reported to have come under a permanent DDoS attack for several days on behalf of Russian hackers, an effort which harmed the ability of the Georgian hacker community to exchange information regarding ongoing cyber events. [53]

Origin of the Attacks

As was the case with Estonia, there is no conclusive proof of who is behind the DDoS attacks, even though finger pointing at Russia is prevalent by the media. There seems to be a widespread consensus that the attacks appeared coordinated and instructed. [54,55]

According to Arbor Networks data traffic analysis, major DDoS attacks observed were all globally sourced, suggesting a botnet (or multiple botnets) behind them.[56]

According to the Shadowserver Foundation from the initial days of the Georgian cyber incident, there were at least six different C&C[57] servers involved in the attacks; some of the botnets operated by them are either "DDoS for hire" or "DDoS for extortion" services which otherwise apparently employ a regular pattern in attacking sites and rarely go after a non-commercial site. [58] The HTTP-based botnet C&C server was reported to be a MachBot controller and as such, a tool that is frequently used by Russian bot herders, and the domain involved with this C&C server had, according to Steven Adair of the Shadowserver Foundation, seemingly bogus registration information which, however, ties back to Russia.[59]

There is some indication of the RBN involvement, which was also referred to earlier in this paper (see 'Other types of attack' under 'Methods of cyber attack')[60]. The security experts of Shadowserver presume that the involvement of RBN did not amount to more than providing hosting services to the botnet C&Cs and it did not commit the DDoS attacks itself.[61]

---

[53] Danchev, *supra* note 29.

[54] Danchev, *supra* note 29.

[55] *See*, e.g., Project Grey Goose. *Supra* note 42, p 4.

[56] According to Jose Nazario, the DDoS attacks were mostly TCP SYN floods with one TCP RST flood in the mix; no ICMP or UDP floods were detected. *See* J. Nazario, 'Georgia DDoS Attacks - A Quick Summary of Observations', *Arbor Networks*, 12 Aug 2008, available at: asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations (last accessed: 14 Aug 2008).

[57] Botnet command and control servers, commonly abbreviated by the IT society as C&C.

[58] Johnson, M. 'Georgian Websites Under Attack - Don't Believe the Hype', *Shadowserver Foundation*, Aug 12, 2008, available at: www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080812 (last accessed: 27 Aug 2008).

[59] Adair, *supra* note 12; G. Craciun, 'President of Georgia Web Page Down after Hacker Attack - The Russians are believed to be behind it', *Security News Editor*, available at: news.softpedia.com/news/President-of-Georgia-Web-Page-Down-after-Hacker-Attack-90420.shtml (last accessed: 27 Aug 2008).

[60] Johnson, *supra* note 58. *See supra* note 51 for an explanation of RBN.

[61] *Id*.

The Project Grey Goose team reports of being unable to find, in their research into the Russian hacker sites, any references to state organisations guiding or directing attacks, be it because there was none, because the collection efforts were not far-reaching or deep enough to identify these connections, or because involvement by state organisations was conducted in a way to purposefully avoid attribution. [62] However, the report refers to historical evidence that past and present members of the Russian government endorse cyber warfare and/or cyber attacks initiated by their country's hacker population.[63]

Also, as was the case with Estonia, there seems to be a wide public understanding that the attacks were at least tolerated by the Russian authorities, if not coordinated or supported by them. Supporting circumstantial evidence can be provided in both cases:

- Both conflicts have as their background a large-scale collision of interests between the country under attack and Russian authorities;

- The coordination of and support to attacks took place mainly in the Russian language and was conducted on Russian or Russia-friendly forums.

Sources indicate a connection between organised crime and the Georgian cyber incidents. According to the above-referred study carried out by the Swedish National Defence University, stopgeorgia.ru is related to different criminal activities, such as forged passports and stolen credit cards, i.e. activities that normally should be prosecuted by the authorities; however, the Russian authorities have remained remarkably passive in prosecuting the person in this particular case.[64] The Project Grey Goose report points out that the stopgeorgia.ru site – which provided information and tools for independent hackers to attack Georgian sites – was hosted by SoftLayer Technologies, Inc. (AS36351) of Plano, Texas, USA, the latter being controlled by Atrivo, a host listed as the 4th worldwide among webhosts capacitating spread of malware, spam, financial scam, and identity theft.[65,66]

Dancho Danchev of ZDNet points out that "an average script kiddie" would not bother nor understand the psyops effect of coming up with identical gestures of Saakashvili and Hitler and integrating them within the defaced sites.[67] It is obvious from some of the attacks the amount of photos and the similarities of gestures presented that putting the collage together demanded time, commitment and resources.

Based on their data collection and analysis, the Grey Goose Project analysts discern a pattern in the Georgian attacks, comprising of 5 stages: spreading encouragement to get

---

[62] Project Grey Goose, *supra* note 42, p 3

[63] *Id.*, pp 3, 6-8

[64] Swedish National Defense University, *supra* note 41.

[65] Armin, J. 'Atrivo – Cyber Crime USA: White Paper - Atrivo and their Associates'. Vers: 1.1, September 2008. Available at: hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf (last accessed 19 Nov 2008)

[66] SoftLayer Technologies - Does the Cyber War "Buck" Stop There?. *Intelfusion*. Available at: intelfusion.net/wordpress/?p=452 (last accessed 19 Nov 2008)

[67] Danchev, *supra* note 29.

involved in the cyber war against Georgia, publishing a target list of Georgian government Web sites which have been tested for access, selection of types of malware to use against the target Web site, launching attack and optionally, result evaluation.[68] The conclusions leave little doubt that the Georgian cyber attacks were largely coordinated, not simply an *ad hoc* reaction of individual cyber-activists sympathetic to the Russian cause. This may constitute a new development compared to the incidents in Estonia, where coordination was recognized only in the second phase of the cyber attacks.[69]

Countermeasures

According to Shadowserver, some of the attacked websites remained online and did not really make any changes to defend themselves. A few of the websites temporarily changed their IP addresses to loop back to the originating network[70] in an attempt to thwart the attacks. A few others also changed hosts.[71]

The interpress.ge news portal moved to Servage (www.servage.net), a worldwide hosting platform provider. Civil.ge, a Georgian news portal, temporarily switched to publishing their news coverage at a Blogger account (civilgeorgia.blogspot.com). Georgia's Ministry of Foreign Affairs also opened a Blogger account (georgiamfa.blogspot.com) for distribution of information.

The websites of the Ministry of Defence and the President were relocated to Tulip Systems, Inc., located in Atlanta, Georgia, the USA, and the website of the Ministry of Foreign Affairs was moved to an Estonian server.[72,73,74]

The Office of the President of Poland provided their website (www.president.pl) for dissemination of information and helped to get Internet access for Georgia's government after breakdowns of Georgian local servers caused by cyber attacks.[75]

Attack mitigation within Georgia was coordinated by CERT Georgia, who normally provides computer and network security technical support to the Georgian higher

---

[68] Project Grey Goose, *supra* note 42, p 5

[69] CCD COE Legal Task Team, *supra* note 3.

[70] This was done by changing the IP to 127.0.0.1 (*localhost*), which is the standard IP address used for a loopback network connection (upon trying to connect to 127.0.0.1, one is looped back to one's own host).

[71] Adair, *supra* note 12.

[72] CERT-EE, *supra* note 31.

[73] Rand, E. Gruusia välisministeeriumi kodulehekülg paigutati Eesti serverisse (*in Estonian*). EPLOnline. August 12, 2008. Available at: www.arileht.ee/artikkel/438306 (last accessed 20 Nov 2008)

[74] According to the information exchanged in a meeting at the Estonian Ministry of Foreign Affairs in September 2008, the initiative of the Estonian Ministry of Foreign Affairs to host the Georgian Ministry of Foreign Affairs website could not have happened, and certainly not in such a short timeframe (the site was reportedly moved within 24 hours), without Estonia learning lessons from 2007.

[75] 'Cenne polskie wsparcie dla Gruzji' (in Polish), *RMF FM*, 9 Aug, 2008, available at: www.rmf.fm/fakty/?id=141305 (last accessed: 27 Aug 2008). *See* also: 'Information about the latest developments in Georgia', *President of the Republic of Poland*, available at: www.president.pl/x.node?id=479 (last accessed: 10 Aug 2008).

education institutions (as a unit part of the Georgian Research and Educational Networking Association, GRENA)[76] and who assumed the role of national CERT during the cyber attacks.[77]

CERT Poland analyzed IP data and sent out abuse messages, while CERT France helped with collecting log files.[78]

From August 12 to 16, two information security specialists from CERT Estonia also visited Georgia in order to assist the local CERT by providing their knowhow and experience.[79]

Effects of the Attacks

CERT-EE has provided information on the two main players on the Georgian Internet access and services market, United Telecom and Caucasus Network. United Telecom of Georgia router (Cisco 7206 series) was unavailable and incapable of providing service for several days.[80] Caucasus Network Tbilisi was flooded with excessive queries; according to data provided to the Estonian CERT by Caucasus Network, rerouting of traffic may have affected the smaller Internet providers.[81] The problem was escalated by the fact that the Caucasus Network infrastructure runs through the war activity zone, which also caused physical disconnections.[82]

The unavailability of crucial websites of the Georgian government caused by the DoS and DDoS attacks severed communication from the Georgian government in the early days of the Georgian-Russian conflict – a period that was doubtless the most critical in the events and where the Georgian government had a vital interest in keeping the information flowing to both the international public and to its own residents. The unavailability of the core state institutions' websites can additionally be seen as serving a discouraging effect on Georgian nationals.

Given the different context of the Georgian cyber event compared to the Estonian cyber attacks in spring 2007, the damage is manifested in different categories as well. Whereas in Estonia, the core of the damage consisted of obstructed access to socially vital

---

[76] 'CERT Georgia'. A description of mission and services is available at: www.grena.ge/eng/cert.html (last accessed 20 Nov 2008)

[77] CERT-EE, *supra* note 26.

[78] *Id*.

[79] 'Eesti aitab Gruusiat küberrünnete tõrjumisel' (*in Estonian*), Estonian Informatics Centre, Aug 12, 2008, available at: www.ria.ee/index.php (last accessed: 27 Aug 2008)

[80] According to CERT-EE, CPU utilization at UTG was 100%, which made it almost impossible to get console access. The cause seemed to be some sort of BGP upload activity. L3 switches on the way to the router were unaffected. *See supra* note 26.

[81] The Caucasus has a 1G backbone and an uplink (probably 3 x STM1) via Turkey and Azerbaijan. Caucasus was reported to have been flooded with 150Mbit/s traffic, TCP SYN flood towards interpress.ge port 80. *Id.*

[82] Danchev, *supra* note 29.

electronic services provided by both the public and private sector, such as e-government and e-banking services, in Georgia, the heart of the damage lied in limiting the nation's options to distribute their point of view about the ongoing military conflict– in "making its voice heard" to the world. Simultaneously, Georgia's own public was deprived of information.

The cyber incidents also had a reflection on the provision of public services. As a consequence of the attacks, on August 9, the National Bank of Georgia ordered all banks to stop offering electronic services. On Monday, August 18, the National Bank reported that all commercial banks in Georgia were back to operating business as usual[83], which, however, meant that electronic banking services were out of function for ten days.[84]

In Georgia's case, the significance of service disruption is different compared to the importance that the spring 2007 cyber attacks had in Estonia, as the scale of the two countries' information and communication technology (ICT) dependence is rather different. As dependence on ICT for everyday services and communication correlates with the level of harm that could be caused by the attacks, generally, countries with a higher degree of ICT development are more exposed to cyber attacks and consequently face greater damage, and the same is true in reversion. Regarding the Georgian case, Josè Nazario (Arbor Networks) was quoted in media as not seeing devastating effects.[85] However, even though the relatively low ICT dependence of Georgia limited the damages caused by the cyber attacks on the service providers, Georgia also illustrates another trend in the effect of cyber attacks: namely, countries whose ICT availability is low suffer most in terms of efficiency of information flow.

The short-term and long-term effect of cyber attacks must also be kept in mind. While the attacks did not have a permanent or even a long-run devastating effect on the Georgian Internet infrastructure, the damage caused by the attacks was most acutely experienced at the time when Georgia was the most dependent on the availability of their information channels. This brings up another characteristic of cyber attacks: unlike the effect of kinetic force, cyber attack can be designed in a way to cause only temporary harm in a particular timeframe.

As is the case with Estonia, the amount of damage caused by cyber attacks is difficult to estimate in monetary categories[86] – even more so in the case of Georgia since the timing of the cyber incidents coincided with physical damages caused by the ongoing armed conflict. A conclusive estimation of damages of cyber attacks would require a systematic

---

[83] 'All commercial banks in Georgia are operating business as usual', *National Bank of Georgia*, Aug 18, 2008, available at: www.nbg.gov.ge/index.php?m=340&newsid=832 (last accessed: 18 Aug 2008).

[84] Compared to Estonia, where online banking services were out of function for two hours, this is a lengthy period. However, given the hight dependence on Estonians on e-banking (over 90% of all banking transactions are conducted via electronic means), even this relatively short timeframe was already considered critical.

[85] Arnoldy, B. Cyberspace: New Frontier in Conflicts. ABC News, 17 Aug 2008. Available at: abcnews.go.com/Technology/AheadoftheCurve/Story?id=5590834&page=2 (last accessed: 25 Nov 2008)

[86] Linnamäe, L. 'Küberrünnakute kahjusid hakatakse arvutama hiljem' (in Estonian). *Postimees*, May 5, 2007. Available at: suusk24.postimees.ee/110507/esileht/majandus/259796.php (last accessed: 20 Nov 2008)

and inclusive effort from all parties involved – government, private sector as well as the users. In many cases, reluctance of the private sector to provide exact data on the kind and size of the damages occurred may be predicted, as there are reasonable and genuine concerns as to the negative effect of revealing such data both in terms of business interest and security considerations; such data may also fall under the protection of business confidentiality, which means that there is no legal obligation to the private sector enterprises to provide data.

In summary, this means that while it is possible to describe the kinds of damages that extensive cyber attacks like those witnessed in Georgia and Estonia may produce, it will be unlikely that exact figures on damages will be available.

However, a discussion of the effects of cyber attacks would not be complete without also taking note of the any benefits that arose from the Georgian cyber incidents, foremost to Georgia, but also to the international community. In this context, international media attention to Georgia, the international cooperation and assistance offered (see above under the subdivision 'Countermeasures'), and international awareness these events have raised, has certainly been beneficial to both Georgia and the international community.

III Legal Lessons Identified from the Georgian Case

The Applicable Legal Regime

In order to determine the authorities' capability to act, the extent of their involvement as well as legal basis for international cooperation, it is necessary specify the legal framework applicable to the cyber incident under question.

The categories of cyber incidents may range from simple deviations from internal regulations and best practices to cyber terrorist acts and cyber warfare. These categories may fall into different legal areas (IT regulatory framework, criminal law, law of armed conflict) and thus are covered under various legal provisions in national and international law.

As regards the Georgian cyber events, the potential applicability of law of armed conflicts (LOAC)[87] is analysed first. We will then focus on the applicability of criminal law and possible legal support under ICT legal framework.

Applicability of International Humanitarian Law

Rationale of questioning the applicability of LOAC

Media has titled the cyber attacks against Georgia as "cyber war"[88] and security experts point out similarities of the Georgian incidents to the cyber events in Estonia in April 2007, a conflict that is frequently referred to as "Cyber War I"[89]. However, in international public law, the term "war" carries a certain legal meaning, triggering a set of rules for the conduct of the parties involved. Bearing in mind that neither a public opinion nor a definition uttered by the media or a politician may not always coincide with the legal categorisation, it is therefore appropriate to analyse whether the cyber attacks against Georgia are subject to the application of LOAC.

It must be noted that LOAC is a term comprising two major sets of rules: *jus ad bellum* that focuses on the criteria for going to war in the first place (covering issues such as right purpose, duly constituted authority, last resort) and *jus in bello* that creates the

[87] International humanitarian law (IHL) is also known as laws of war or law of armed conflict (LOAC). In this analysis the terms are used interchangeably as synonyms.

[88] E.g. Markoff, J. 'Before the Gunfire, Cyberattacks'. *New York Times*, 13 Aug 2008. Available at: www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&em (last accessed 20 Nov 2008); Swaine, J. Georgia: Russia 'conducting cyber war'. *Telegraph*, 11 Aug 2008 Available at: www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html (last accessed 20 Nov 2008)

[89] M. Landler, J. Markoff, 'In Estonia, what may be the first war in cyberspace', *The International Herald Tribune*, May 28, 2007, available at: www.iht.com/articles/2007/05/28/business/cyberwar.php (last accessed: 27 Aug 2008).

concept of just war-fighting (covering non-combatant immunity, proportionality etc.). Due to the level of abstraction of this paper the term LOAC is used without referring to neither of them in particular. Wherever only certain aspects of LOAC are referred to, they are pointed out.

General prerequisites for the applicability of LOAC

In order for LOAC to apply to a particular armed conflict, neither formal declaration of war, nor recognition of a state of war is required. Instead, the requirements of LOAC become applicable "as from the actual opening of hostilities" *(ex nunc)*.[90] An international armed conflict is perceived as "[a]ny difference arising between two States[91] and leading to the intervention of armed forces… even if one of the Parties denies the existence of a state of war".[92] The *de facto* situation between Georgia and Russia in August 2008 involved armed forces in operation in a cross-border conflict, beyond the area where the peacekeeping mandate was applicable. Thus, even though the Georgian declaration of a "state of war" (referred to in section 'Background and Context…' of this paper) was an internal measure rather than one based on international law, and regardless of the claims of Russia that it only entered the territory of Georgia in order to "defend the lives and dignity of its citizens" in South Ossetia and Georgia, describing its intervention as a peacekeeping operation[93], the applicability of LOAC to the Russian-Georgian conflict raises few doubt.[94]

---

[90] The authoritative Commentary of the International Committee of the Red Cross on the 1949 Geneva Conventions states that "[t]here is no longer any need for a formal declaration or war, or for recognition of the state of war, as preliminaries to the application of the Convention. The Convention becomes applicable as from the actual opening of hostilities." *See* J. Pictet (ed.), *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, ICRC, Geneva, 1952, p. 32.

[91] Nevertheless, after the terrorist attacks of 11 September 2001 in the United States, the international community has acknowledged the changes regarding parties in armed conflict. The terrorist attacks against the United States were conducted by the terrorist network al-Qaeda led by Osama bin Laden and were considered armed attacks both by the UN and NATO. In addition, US president George W. Bush also held the Taliban regime of Afghanistan responsible for the attacks because it allowed al-Qaeda to operate on Afghanistan territory. After the attacks on the World Trade Center in New York, US President started his War on Terror which was first demonstrated by the invasion into Afghanistan by the troops of the USA and several of its allies. Hence, the attacks of 11 September 2001 expanded the traditional definition of armed conflict, e.g. armed conflict does not necessarily have to arise between two States but instead one of the parties can be, for example, a private group supported by a state. In this case, the question of state attribution and state responsibility arises.

[92] Pictet, *supra* note 90.

[93] Statement of the President of Russia on August 8, 2008. Medvedev, D. 'Statement on the Situation in South Ossetia', August 8, 2008 available at: www.kremlin.ru/eng/speeches/2008/08/08/1553_type82912type82913_205032.shtml (last accessed 02 Sept 2008) In his statement, the President relied on the Constitution of the Russian Federation to justify the interference in Georgia, as Article 80 (2) of the Constitution stipulates "The President of the Russian Federation shall be guarantor of the Constitution of the Russian Federation, of the rights and freedoms of man and citizen. According to the rules fixed by the Constitution of the Russian Federation, he shall adopt measures to protect the sovereignty of the Russian Federation, its independence and state integrity, ensure coordinated functioning and interaction of all the bodies of state power.", *See* The Constitution of The Russian Federation, available at: www.constitution.ru/en/10003000-01.htm (last accessed 27 Aug 2008).

[94] This position is shared by e.g. Human Rights Watch ('Q & A: Violence in South Ossetia'. *Human Rights Watch*. 15 Aug 2008. Available at: www.hrw.org/en/news/2008/08/15/q-violence-south-ossetia, last accessed 20 Nov 2008); Council of Europe Parliamentary Assembly Resolution 1633 (2008) on 'The consequences of the war between Georgia and the

This does not, however, automatically mean that LOAC would also be applicable to the cyber attacks that took place simultaneously with the physical attacks potentially to be regarded as armed conflict. Both the notions of "cyber war" and "cyber attacks" must be assessed in legal terms; it must be examined whether the cyber incidents in Georgia satisfy the criteria of an "armed attack" that triggers the applicability of *jus in bello*.

As stated above, the involvement of armed forces in the conflict is an important prerequisite for the applicability of LOAC. As regards cyber incidents, many countries have not created a specific "cyber force" in their military command, a fact that makes such a connection practically impossible. With reference to Schmitt[95], the engagement of armed forces cannot be the sole decisive criterion. Schmitt explains: At the time when the [LOAC] instruments were drafted, armed forces were the entities that conducted [armed attacks].[96]

According to Schmitt, the most important detail is the nature and, more importantly, the effect of the conduct under question. Based on the reasoning established for defining traditional armed conflicts, an action can be defined as an 'armed attack', thus triggering the applicability of LOAC, if that action is either intended to cause injury, death, damage or destruction, or such consequences are foreseeable.[97] According to Solce[98], cyber terrorism and cyber warfare would constitute cyber attacks in the context of LOAC.

To make use of Solce's argument, it is necessary to next examine whether the incidents in Georgia meet the criteria listed above. When evaluating the consequences of computer attacks, both the physical and mental sides must be taken into account. Economic harm and loss of tangible property can be considered as damage and destruction; significant human physical and mental suffering is logically included in the concept of injury.[99] Mere inconvenience, harassment or diminishment in the quality of life does not reach the level of injury or damage. It is a matter of estimating the level of human suffering to decide whether a certain cyber incident would constitute an attack within the definition of an attack in terms of humanitarian law.[100]

With reference to subsection 'Effects of the attacks' in this analysis, the direct effect of the cyber attacks is difficult to estimate. Whereas negative implications on access to

---

Russian Federation', available at assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta08/ERES1633.htm (last accessed 20 Nov 2008)

[95] Schmitt, Michael N. Wired Warfare: Computer Network Attack and *jus in bello*, IRRC June 2002, Vol. 84, No. 846, page 372 ff.

[96] *Id*.

[97] See, e.g. Schmitt, *supra* note 95.

[98] Solce, N. 'The Battlefield of Cyberspace: the Inevitable New Military Branch – the Cyber Force'. In: 18 ALB. L.J. Sci. & Tech. 293 2008,

[99] Schmitt states that is it reasonable to include human suffering in the connotation since the Protocol prohibits causing terror, which is also a psychological condition. Art. 51 (2) Additional Protocol I to the Geneva Convention, 1997. Schmitt, *supra* note 95.

[100] *Id*.

information and information society services are evident, the extent of monetary loss and human suffering is difficult to calculate.

Although in the Estonian case, where conviction followed under provision 207.2[101] of the Penal code, assuming "major damage"[102], it must be noted again that in spite of the terminology, the findings of the court only support the criteria of damage set under criminal law pertaining to computer crime.

It is difficult to determine that the cyber incidents in Georgia constitute a breach of what can be regarded as state's international duty. In order to hold a state responsible for cyber attacks under LOAC, it must also be established that the cyber attacks can be directly connected with a particular state (state attribution).

The governing principle of state responsibility under international law has been that the conduct of private actors – both entities and persons – is not attributable to the state, unless the state has directly and explicitly delegated a part of its tasks and functions to a private entity.[103] A shift in this rigid paradigm can be observed in the developments of recent years: e.g. the International Criminal Tribunal for the former Yugoslavia in the *Tadic* case[104] and further by the international community in relation to the U.S. Operation Enduring Freedom in 2001.[105] However, the current view for attribution still requires some form of overall control by the state.

---

[101] § 207 (2) of Estonian Penal Code stipulates that unlawful interference or hindrance of the operation of a computer system by way of entry, transmission, deletion, damaging, alteration or blocking of data is punishable by a pecuniary punishment or up to 5 years' imprisonment if significant damage is thereby caused or the operation of a computer system of a vital sector (critical infrastructure) or the provision of public services is thereby hindered.

[102] According to Implementation Act of the Estonian Penal Code (§ 8), in the legal assessment of offences pursuant to the provisions of the Penal Code or another Act which prescribes the causing of damage as a constituent element, proprietary damage shall be assessed as follows: 1) damage exceeding ten times the established minimum monthly wage is significant damage; 2) damage exceeding one hundred times the established minimum monthly wage is major damage (In 2008, the minimum monthly wage in Estonia is 4350 *kroons* = 278 €).

[103] In the *Nicaragua* case, the International Court of Justice (ICJ) noted that the state may be held responsible for the conduct of private actors only *if it executed effective control over such actors*. Hence, the ICJ could not hold the United States responsible for the conduct of the *contra* rebels, because the United States did not exercise effective control over the contras. The Court also noted that, in order for the conduct of private actors to give rise to legal responsibility of the state, it would have to be proved that the state indeed had effective control over the conduct of private actors. *See Military and Paramilitary Activities in and against Nicaragua* – ICJ Reports, 1986; Jinks, D. 'State Responsibility for the Acts of Private Armed Groups', *Chicago Journal of International Law*, 4 (2003), 83-95, p. 88.

[104] In comparison with the Nicaragua case and the ICJ rule, the ICTY in the *Tadic* case lowered the threshold for imputing private acts to states and concluded that states only need to exercise *overall control over private actors* in order to attribute to the state any unlawful acts of the actors. The ICTY in its reasoning held that the 'effective control' criterion of the ICJ was contrary to the very logic of state responsibility and that it was inconsistent with state and judicial practice. See *Prosecutor* v. *Tadic* - ICTY Case No. IT-94-1, 1999.; Jinks, p. 88-89.

[105] Compared to the *Tadic* case, the U.S. Operation Enduring Freedom in turn lowered the threshold for attribution because the U.S. sought to impute al Qaeda's conduct to Afghanistan simply because its official regime Taliban had *harboured* and *supported* the terrorist group (irrespective of whether Afghanistan exercised effective or overall control). The international community among with several important international organisations endorsed the U.S approach and determined that under international instruments the attacks of September 11 constituted armed attacks which triggered the U.S inherent right of self-defence. The U.N, NATO and the OAS also attributed the terrorist attacks of al Qaeda to the Taliban regime. *See* Jinks, *supra* note 103, p. 85-87.

The law of state responsibility is based on the concept of agency. Hence, in determining whether responsibility can be attributed to a state, the key questions are (a) whether a person has acted as an agent of a particular state and (b) whether his actions qualify as actions of that state.[106] Contrary to what is the case when a state is directly exercising its public functions, it is hardly possible to demonstrate that a state is responsible for the acts of private parties.[107] In those cases, the state does not bear direct responsibility for private acts, but can instead bear indirect responsibility, meaning that the state can be held responsible for tolerating the private action in question or for being incapable of preventing it.[108]

The rules governing state responsibility were codified in 2001 into the Draft Articles on Responsibility of States for Internationally Wrongful Acts,[109] which can be considered as a reflection of *customary international law* – the latter being binding upon all states.[110] According to article 12 of the Draft Articles, a breach (that entails liability under international law) occurs when an act of a state does not conform to what is required of that state by the particular obligation under international law, regardless of the origin or character of said act. What is considered an internationally wrongful act is determined by international law.[111]

There is currently no universal legally binding instrument that would address cyber attacks as threats to *national security*.[112] Even though some states have adopted non-binding instruments at organisational level, these documents can be viewed as general guidelines with limited applicability and without any foreseen sanctions in the case where states do not adhere with the set out principles.[113]

---

[106] Under international law, the conduct of formal state organs and their officials is usually attributable to the state (as they have been authorised by the state to exercise public functions) and therefore it is considered that the state itself has committed that act. Whereas the conduct of private actors, both entities and persons is attributable to the state, when it is sufficiently connected with the exercise of public functions. *Id.*

[107] Because the state is responsible for its wrongdoings and regards to private breaches, the state has the duty to prevent or abstain from supporting private perpetrators. *Id.*

[108] This is the case in state-on-state situations, e.g. the private actors are still responsible before the state for breaching their obligations arising from national legislation.

[109] Draft as on 15 September 2008.

[110] General Assembly Resolution 58/63, 28.01.2002, Annex (Draft Articles). *See* René Värk 'State Responsibility for Private Armed Groups in the Context of Terrorism', XI *Juridica International*, 2006, 184-193, p. 185.

[111] Värk, *supra* note 110, p. 185.

[112] The best known document that directly addresses threats arising from cyberspace and the Internet is the Council of Europe Convention on Cyber Crime. Organisations such as the UN, NATO, OECD, and the EU have also adopted instruments that focus on fight against cyber crime and terrorism as well as on the need for secure state information systems and the need to protect critical (information) infrastructure.

[113] Of course, this would not be the situation if a cyber attack would constitute an armed attack within the meaning of Article 51 of the UN Charter. In this case, a state would be responsible for breaching its international duty deriving from Article 2 (4) of the Charter which stipulates that "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the UN". It should be noticed, that the violation of the UN Charter automatically entails the violation of General Assembly Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations 1970 Article 1. *See* D.J. Harris, *Cases and Materials on International Law*, 6th ed, London: Sweet & Maxwell, 2004, p. 1090, 1121.

As previously discussed, in neither the Georgia 2008 case nor in the Estonia 2007 case preceding it has it been possible to prove support by any certain state behind the cyber attacks.

In conclusion, it is highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks – the objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect. Therefore, the potential remedies arising from Geneva Conventions and IHL in general, as well as their usefulness, remain beyond the scope of this analysis.

Applicability of National and International Criminal Law

Rationale of questioning the applicability of criminal law

As information technology has evolved, many countries have included provisions of computer crimes in their criminal law to fight the disturbing trends of identity theft, intrusion into networks and spread of viruses. In 2001, the Council of Europe adopted the first international agreement in the field – the Cyber Crime Convention[114] that contains both substantial and procedural aspects of investigating cyber crimes. Therefore, it is relevant to consider the legal framework applicable in Georgia in terms of criminal law.

Georgia signed the Council of Europe Convention on Cybercrime in April 2008 but has, as of August 2008, not yet ratified the convention. Russia has neither acceded to nor ratified the convention. Estonia had ratified the Convention already before the Estonian cyber attacks took place, but the investigation of the incidents indicated some legal loopholes so the law had to be revised.[115]

---

[114] Convention on Cybercrime, Council of Europe, ETS 185, available at: conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (last accessed: 27 Aug 2008).

[115] As a result of the revisions, the Penal Code regulation concerning computer related fraud with the liability of legal person was amended. Another big amendment was related to the preparation of computer crimes. Currently, § 216[1] of the Penal Code foresees a liability for the preparation of computer crimes concerning data intervention, prevention of computer system process, spreading of computer viruses, computer-related fraud, and illegal use of computer system. Article 237 of the Penal Code was also amended in a way where a computer attack would become an act of terrorism when it is committed with the same aims as a conventional act of terrorism. In comparison with the previous regulation, the terms of sentences were also increased in some cases, for example for data intervention: earlier - fine or up to one year of imprisonment, now – fine or up to three years of imprisonment.
The Parliament of Estonia passed the Act to Amend the Penal Code on 21 February 2008 and the amendments entered into force on 24 March 2008. See Pikamäe, T. "Changes in Penal Code," June 2008. Available at: www.infolex.lt/portal/ml/start.asp?act=legupd&lang=eng&biulid=144 (last accessed: 25 Nov 2008); see also The Baltic Times "Estonia Gets Tough on Cybercrime," 17 Sept, 2007. Available at: www.baltictimes.com/news/articles/18815/ (last accessed: 25 Nov 2008).

Georgian Criminal Law in the Field

Since the Convention on Cybercrime has not entered into force for Georgia, investigation of the incidents must be based on Georgia's national material and procedural law. The following analysis is not intended to cover all aspects of Georgian national law and only highlights the key elements worthy of consideration in deciding on further action.

Under chapter 47 ("Computer Crime") of Georgian Criminal Code [116], unlawful infiltration into the computer information (Art. 303), creating, applying and disseminating a program damaging computers (Art. 304), and infringement of the rules for exploiting computers, computer systems or their networks (Art. 305) is prohibited and punishable. [117] Thereby, Georgian authorities are, in principle, in a position to instigate criminal proceedings to investigate the cyber attacks that took place in August 2008.

In the Estonian case, a successful conviction derived from § 207 (2) of the Penal Code, whereby unlawful interference or hindrance of the operation of a computer system by way of entry, transmission, deletion, damaging, alteration or blocking of data is punishable by a pecuniary punishment or up to 5 years' imprisonment if significant damage is thereby caused or the operation of a computer system of a vital sector (critical infrastructure) or the provision of public services is thereby hindered.

Taking the assumption that the same deeds are punishable also in (at least some of) the countries that the attacks originated from – which is the prerequisite for international criminal cooperation with those countries – Georgia may lean on the provisions of international criminal cooperation conventions of the Council of Europe. Nearly all of the 47 Council of Europe member countries, including Georgia and Russia, have acceded and ratified the European Convention on Mutual Assistance in Criminal Matters and Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters.[118]

---

[116] The CCD COE Legal Task Team received the text of Georgian Criminal Code from Academy of the Ministry of Internal Affairs of Georgia via the OSCE Mission in Georgia; the authors of this paper cannot ensure that the provisions of the Georgian Criminal Code cited in this paper are up-to-date.

[117] According to the Georgian Criminal Code: Unlawful infiltration into the computer information, or the information reflected in the computer network system, if this action destroyed, blocked, modified or copied the information, or disrupted the work of computers, computer systems or networks, are punishable by a penalty to from 70 to 360 times the daily salary or correctional work for a period of up to two years, or deprivation of liberty for the same period. According to Art 303 (2), the same action committed by a group by a prior agreement, are punishable by a penalty equal to 240 to 360 times the daily salary or correctional work for a period of up to five years, or imprisonment for a period of up to four months, or deprivation of liberty for a period of up to five years. Under Article 304, creating a program damaging computers or making changes in existing programs that intentionally cause unsanctioned destruction, blockage, modification or copying of information, disruption of the work of computers, computer systems or network, are punishable by a penalty equal to from 100 to 360 times the daily salary or correctional work for a period of up to three years or deprivation of liberty for the same period.

[118] European Convention on Mutual Assistance in Criminal Matters. Council of Europe. CETS No.: 030 available at: conventions.coe.int/Treaty/EN/Treaties/Html/030.htm (last accessed: 02 Sep 2008);

Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. Council of Europe. CETS No.: 099; .available at: conventions.coe.int/Treaty/EN/Treaties/Html/099.htm (last accessed: 02 Sep 2008)

According to Article 1 of the Convention, the contracting parties undertake to afford each other "the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party". According to Article 3.1, the requested Party shall execute in the manner provided for by its law any letters relating to a criminal matter and addressed to it by the judicial authorities of the requesting Party for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents. Assistance may be refused, under Article 2, only if the request concerns an offence which the requested Party considers a political or fiscal offence or an offence connected with a political offence (as for Russia, it has made a declaration to the convention defining the characteristics of crimes it may consider as such), or if the requested Party considers that execution of the request is likely to prejudice the sovereignty, security, *ordre public* or other essential interests of the country. Any refusal for mutual assistance must be motivated. In accordance with Article 26, the Convention supersedes the provisions of any treaties, conventions or bilateral agreements governing mutual assistance in criminal matters between any two Contracting Parties.

However, as the legal lessons learned from the cyber attacks against Estonia in 2007 have demonstrated, even existing treaties on legal cooperation may be insufficient for carrying out effective investigation. The efficiency of such treaties is very much tied to the nations' willingness to cooperate and, as is the case with public international law in general, no effective mechanism for sanctions exists should a nation refuse to comply with an international obligation.[119]

As regards national material law, one of the first steps that Georgia could consider taking would be to ratify the Council of Europe Cyber Crime Convention, which at least ensures basic international cooperation in the field of cybercrime. However, given the fact that Russia, which is one of the nations of most interest to Georgia in the investigation of the August 2008 cyber incidents, has not acceded to the Cybercrime Convention and has announced its intent not to ratify the convention[120], Georgia's future ratification of the Cybercrime Convention will not avail too much concerning the cyber attacks under study.

Applicability of ICT Legal Framework

The 2007 Estonian legal lessons learned indicate that one strength Estonia had in coping with and recovering from the attacks, lies in a systematic and well-developed ICT legal framework that sets the standards for IT security. As countries and their legal systems are unique and a thorough analysis of Estonian law would be well beyond the scope of this analysis, it will be useful to point out the basis for this regulation in European Union

[119] Tikk, E., Kaska, K. Russian refusal for cooperation in criminal proceedings: analysis and proposals. April 2008. In Estonian.

[120] Putin defies Convention on Cybercrime. *Computer Crime Research Center*, March 28, 2008. www.crime-research.org/news/28.03.2008/3277/

(EU) countries. The reason for it is that more than any other international organisation, the EU has developed an ambitious and regulated information society.

Georgia has, in recent years, put much effort into modernizing the country's ICT regulation and policy, by *inter alia*, developing an electronic communications legal framework and draft legislation in the field of data protection, based on the key elements of EU principles.[121] Even though Georgia is neither an EU member state nor a candidate country, the nation has expressed their aspiration towards integration to the European Union and sees membership as a long-term goal.[122] Furthermore, the EU and Georgia have a bilateral Partnership and Cooperation Agreement (PCA) since 1999, and Georgia is part of the European Neighbourhood Policy (ENP) program which sets ambitious objectives for partnership with neighbouring countries based on commitments to shared values, key foreign policy objectives and political, economic and institutional reforms, including reforms in the information society segment. The latest ENP Action Plan, endorsed by the EU-Georgia Cooperation Council of 14 November 2006, aims at fulfilling the provisions of the PCA and involves a significant degree of economic integration and political co-operation. As such, EU law in the field of information society and electronic communications is highly relevant for Georgia.

There are several legal mechanisms in EU law that oblige both the state and private actors to maintain a sufficient level of network and information security and could prove to be an efficient example for Georgia in further developing the country's IT legislation.

The electronic communications directives[123] serve as cornerstones for ICT regulation in the EU. Whereas their immediate influence on security of the networks is not evident, they provide for a sustainable and balanced ICT infrastructure and facilitate provision of electronic services in the market.

A general obligation for the service provider to take appropriate technical and organisational measures to safeguard security of its services derives from article 4 of ePrivacy Directive 2002/58/EC[124].

---

[121] Hardabkhadze, Kvernadze, *supra* note 25, pp 6-7.

[122] European Union External Relations: Georgia. *European Commission*. Available at: ec.europa.eu/external_relations/georgia/index_en.htm (last accessed 20 Nov 2008)

[123] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24/04/2002 pp. 0033-0050; and four specific Directives: Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)

[124] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications*);* OJ L 201, 31/07/2002 pp. 0037 – 0047

According to the ePrivacy Directive, ensuring appropriate technical and organisational measures to safeguard security of services is primarily the service provider's responsibility. If necessary (and with respect to the security of the network upon which the service provider's services are provided), the service provider must draw upon help from the provider of the public communications network whom it is connected to. The technical and organisational measures must accord to the *regular risk level* presented to the services and network, however, in case of a *particular risk* of a breach of the security of the network, the service provider is presented an elevated requirement to inform its subscribers concerning the risk and any possible remedies if the service provider cannot neutralise such risks itself.

Users and subscribers must also be informed, free of any extra charge, of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies.

Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. In practice, national legislation in some Member States only prohibits intentional unauthorised access to communications.

Another set of rules that serve as "legal security standard" are the personal data protection principles set forth in the Personal Data Protection Directive 95/46/EC[125]. This Directive provides for terms of exchange of personal data between public and private authorities, potential claims of data subjects as well as the security measures to be taken by data controllers. Proper implementation of these rules will create a clear understanding of the terms of using data available about the incidents for purposes of investigation and further prevention.

Also, implementing the EU Data Retention Directive 2006/24/EC[126] could facilitate investigation of cyber attacks, as the core initiative of the directive is to mandate the European Union member states to set up a national framework to require Internet Service Providers (ISPs) and phone companies to keep data – for a period between six months and two years – on every electronic message sent and phone call made. Even though Georgia is neither an EU member state nor a candidate country, the nation has expressed their aspiration towards integration to the European Union and sees membership as a long-term goal.[127] Thus, the European Union model for data retention might be suitable for consideration for Georgia. Implementing measures stipulated in

[125] OJ L 281, 23 Nov 95, pp. 31-39

[126] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. OJ L 105 , 13/04/2006 pp. 0054 – 0063, available at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (last accessed 27 Aug 2008).

[127] European Union External Relations: Georgia. *European Commission*. Available at: ec.europa.eu/external_relations/georgia/index_en.htm (last accessed 20 Nov 2008)

the Data Retention directive would provide a legal basis to collect the data necessary for investigation of cyber attacks. Of course, this would only be of help for any future incidents.

There are more instruments that will support a solid legal framework in the field of IT security – Directive 2000/31/EC on E-Commerce sets the standards for information society service providers and

Apart from legal regulation it could be beneficial to become a member of the International Organisation for Standardization (ISO). Georgia is currently a correspondent member and does not yet have a fully-developed national standards activity. [128] Although ISO membership does not involve legislative power, the organisation provides instructions to strengthen information security and its membership is an indicator of a certain level of IT security development.

The list of useful initiatives in the EU is much longer. We will therefore only conclude that based on these instruments many countries have built a well-balanced and adapted IT-regulation that for Estonia meant the ability of different authorities to quickly analyse, coordinate and defend against the attacks.

[128] ISO members, available at: www.iso.org/iso/about/iso_members.htm (last accessed: 27 Aug 2008)

IV Conclusions

Effective response means to cyber attacks of scale and type like Georgia obviously are quite limited under law. Most importantly they include the promotion of effective international cooperation as there is no way for a country to coordinate defences against attacks originating from other jurisdictions. It must be kept in mind, however, that virtually no national or international entity has the authority to legislate in the field – national efforts will have to work together with international instruments in different fields and with different focus.

Based on the legal lessons identified and learned from recent public cyber attacks (Estonia 2007, Lithuania 2008, Georgia 2008), it seems that a contemporary "Eastern European" way of cyber-attacking a country is to use the "gray area" in law that does not invoke LOAC. Mostly, the perpetrators operate in a domain that triggers application of relevant provisions in criminal law, which is poorly developed in many countries and has unsolid ground for cross-border cooperation.

It will take time to reach additional consensus on cyber defence legal aspects on international level. Thus far, only 23 countries have ratified the Cyber Crime Convention and only few have been in the position to truly test their national defences in terms of law. Furthermore, the concerns and preparedness of countries in the field of cyber security are different. The lack of experience and the perception of threat are the key reasons why it takes additional time to develop international consensus on these matters.

From a legal point of view, given the current and projected future threat environment (increasing threat of asymmetric attacks by non-state entities, less threat of state-sponsored warfare), there is an increasing likelihood of "grey area" attacks. In fact, it is the general murkiness of this grey area—the lack of clear policies and procedures, the lack of direct evidence of the attacking entity's identity—that may make such "grey area" attacks even more attractive. In such a perceived environment, by deliberately remaining below the threshold of "use of force," an attacking entity may believe there is less likelihood of reprisal even if the attacker's identity is suspected.

Therefore, ratification of cyber crime convention even by all EU or NATO nations does not solve the practical problems related to cyber attacks. Those countries that have witnessed and experienced cyber attacks, have also recognized that there are significant restrictions as regards the applicability and usefulness of cyber crime provisions to such attacks – often the provisions are incomplete, the punishments are weak or the investigatory powers are insufficient. Thus, the relevance of the Cyber Crime Convention cannot be underestimated, but this instrument in its current wording and background as well as status is not the ultimate answer to the problems related to cyber incidents.

As cyber attacks against nation states obviously become more frequent [129], new approaches to traditional LOAC principles need to be developed in order to provide effective legal remedies under this area of law. Although the Geneva Convention does not explicitly define armed conflicts as to include cyber attacks, the latest developments in information warfare welcome such interpretation. Furthermore, the new bloodless types of warfare make estimating the level of suffering difficult and the definition of an "attack" should not be strictly connected with established meanings of death, injury, damage and destruction. Instead the definition of an attack should be consequence-based and bear in mind the final effect on the population.

As current LOAC legislation is hardly applicable to cyber attacks under question and states often get tangled into applying international and national criminal law resulting from the unwillingness of states to co-operate, the best way for international community to protect their IT infrastructures, is through the development and enhancement of their ICT legal framework.

To achieve this goal it is useful to rely on what is there in national and international law that nations can use in order to achieve the goals of international[130] and national cyber defence strategies and policies. Therefore, it is important to determine which best practices there are that individual nations, entities and organizations use and which have helped them to prevent, detect or investigate cyber attacks. Based on these best practices, a check-list for legally supported measures of cyber defence can be created. Such a check-list would enable nations to conduct analysis of their national law and decide which additional legal measures they need to take in order to provide effective defence in event of a cyber attack. Countries that have the development of IT-based services as a key priority for future progress should pay closer attention to legal protection mechanisms concerning information security and possible cyber attacks.

At the same time, legal mechanisms need to be established for national and international authorities' involvement in a cyber incident. To avoid long reaction time and unclear action lines, it must be analysed, what determines the relevance of a cyber incident for particular authorities. This will provide input for nations as to what national procedure they need to follow to determine this relevance and what entities are responsible for analyzing and managing such incidents. Currently, a lot of confusion is created by the fact that virtually all cyber attacks are referred to as 'cyber war' and 'cyber terrorism', which in legal terms cannot be the case until a relevant legal framework is created under national or international law. Not every deviation of everyday IT-security can be regarded as a terrorist act or even a criminal act. In some cases, we deal only with breaches of IT security legislation. That is not to say that there is no need for a legal basis for categorizing a cyber attack as a terrorist attack. The Estonian lessons learned included adding a relevant provision in the Penal Code.

---

[129] See annex VI for an overview of conflicts that have occurred in 2007-2008.

[130] Among the latest aspirations in the field of enhancing international cyber defence strategies and policies is the NATO Policy on Cyber Defence. The policy was approved by NATO Nations in January 2008 and it sets forth the principles for development of NATO's cyber defence capabilities thus strengthening the key information systems of the Alliance and its nations against cyber attacks.

It must be recognized that contemporary cyber attacks do not occur in the domain of LOAC. At the same time it cannot be concluded that they have no relevance for international security and defence purposes. The stability or security of a nation can be shaken by affecting (private) critical information infrastructures.

To be efficient in responses to cyber attacks of relevance, nations and international organisations need additional expertise in the field to provide correct political framework and legal coverage for cyber defence purposes.

The determining factor for the effect of cyber attacks against a country is not only the scale of the country's information and communication technology (ICT) dependence. Dependence on ICT for everyday services and communication correlates with the level of harm that could be caused by the attacks: generally countries with a higher degree of ICT development are more exposed to cyber attacks and consequently face greater damage. The Georgian case clearly shows that countries whose ICT availability is low, suffer most in terms of efficiency of information flow.

Annex I: Facts about South Ossetia[131]

GEOGRAPHY:

South Ossetia is a territory of about 4,000 sq km² about 100 km north of the Georgian capital Tbilisi, on the southern slopes of the Caucasus Mountains.

SEPARATISM:

The collapse of the Soviet Union spurred a separatist movement in South Ossetia, which had always felt more affinity with Russia than with Georgia. It broke away from Georgian rule in a war in 1991-92 in which several thousand people died, and maintains close ties with the neighbouring Russian region of North Ossetia, on the north side of the Caucasus. The majority of the roughly 70,000 people is ethnically distinct from Georgians, and speak their own language, related to Farsi. They say they were forcibly absorbed into Georgia under Soviet rule and now want to exercise their right to self-determination. In 1991, South Ossetia claimed independence from Georgia but has never been accepted as an independent state by international community and has thus remained a *de facto* independent republic. The situation changed somewhat on the 26th of August, 2008 when Russia was the first UN member to *de jure* recognize the independence of South Ossetia. On 3 September, 2008, the Russian example was followed by Nicaragua; currently, these are the only two states that have recognized South Ossetia as an independent state and not as an autonomous region of Georgia. The separatist leader is Eduard Kokoity. In November 2006, villages inside South Ossetia that are still under Georgian control elected a rival leader, ex-separatist Dmitry Sanakoyev. He is endorsed by Tbilisi, but his authority only extends to a small part of the region.

RUSSIAN SUPPORT:

Around two-thirds of annual budget revenues of approximately $30 million (15.5 million pounds) come directly from Moscow. Almost all of the population hold Russian passports; the Russian rouble as their currency. Russia's state-controlled gas giant Gazprom is building new gas pipelines and infrastructure, worth some 15 billion roubles (324.5 million pounds), to supply the region from Russia.

CONFLICT:

A peacekeeping force with 500 members each from Russia, Georgia and North Ossetia monitored the truce. Georgia has accused the Russian peacekeepers of siding with the separatists, which Moscow has denied. Sporadic clashes between separatist and

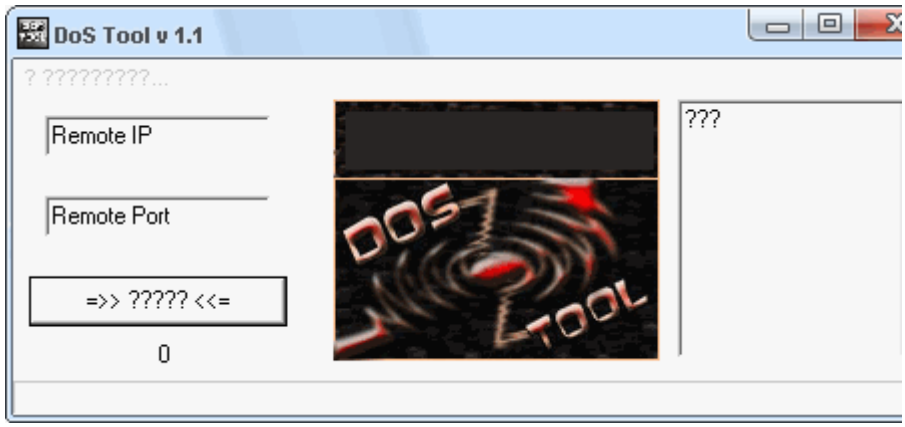
[131] *Sources: Reuters* uk.reuters.com/article/idUKL85578502008080 8?sp=true (last accessed: 27 Aug 2008); Facts about South Ossetia, *The Associated Press*, August 8, 2008; South Ossetia at a Glance, *International Herald Tribune* www.iht.com/articles/ap/2008/08/08/news/Georgia-South-Ossetia-Glance.php (last accessed: 12 Nov 2008)

Georgian forces have killed dozens of people in the last few years. Georgian President Mikheil Saakashvili has proposed a peace deal under which South Ossetia would be given “a large degree of autonomy” within a federal state. The separatist leaders have said they want full independence.

Annex II: Attacks Illustrated

Defacement attack on the Georgia Ministry of Foreign Affairs website (evening of Aug 8, 2008): a collage of photos posted.[132]

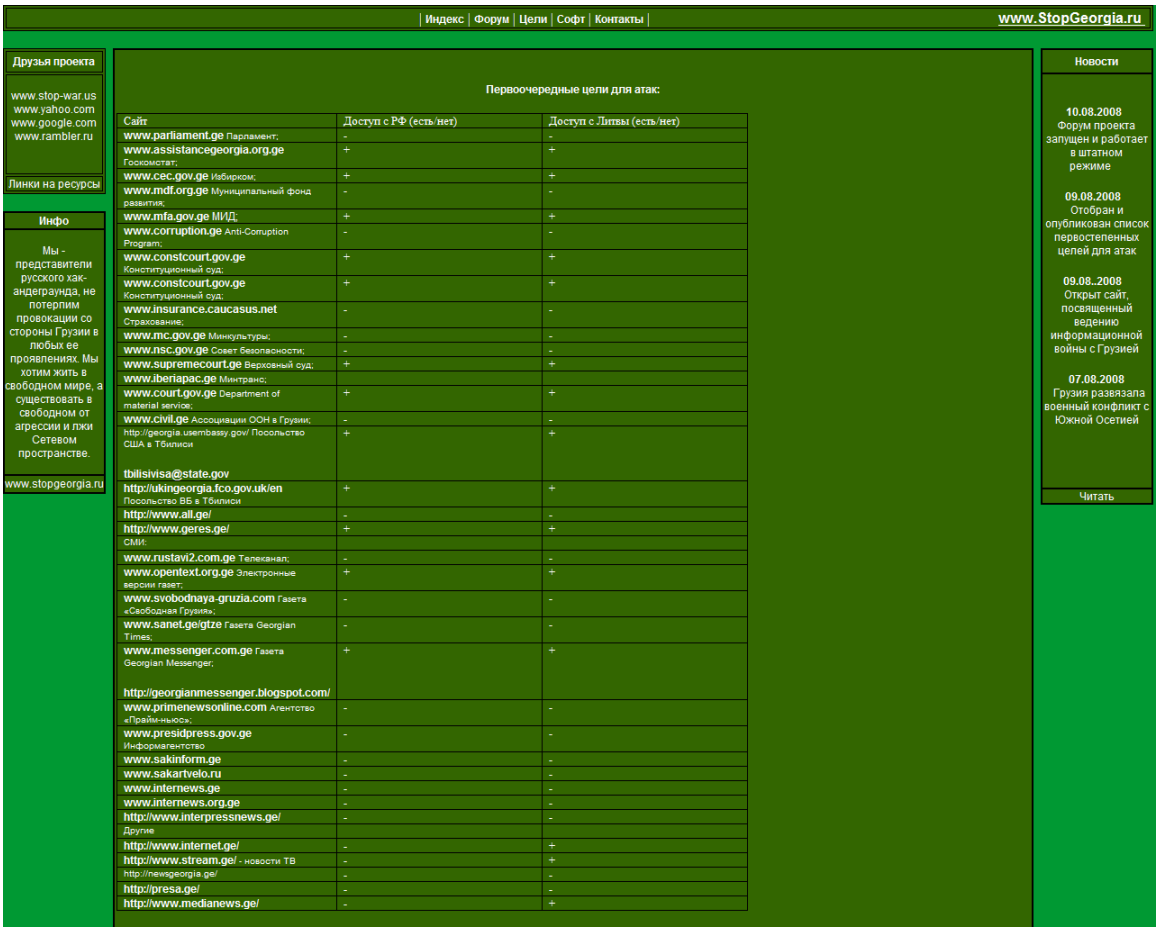
An illustration of a simple HTTP flooder distributed for regular internet users for the purpose of overloading Georgian websites with traffic.[133]



[132] Danchev, *supra* note 29.

[133] Illustration provided by D. Danchev, *supra* note 29. Danchev comments: "Following a basic cyber warfare rule, that the masses are sometimes more powerful than the botnet master's willingness to sacrifice hundreds and thousands of his bots, the current campaign has also thought of the average Internet users who are encouraged to use a plain simple HTTP flooder distributed for this purpose. The concept is nothing new; in fact, this is state of the art cyber warfare combining all the success factors for total outsourcing of the bandwidth capacity and legal responsibility to the average Internet user."

A screenshot from the Stopgeorgia.ru site on August 10, 2008. The table shows the availability of different websites from Russia and Lithuania; the line over the table reads “priority targets for attack”.[134]



| Индекс | Форум | Цели | Софт | Контакты | www.StopGeorgia.ru

Друзья проекта

www.stop-war.us
www.yahoo.com
www.google.com
www.rambler.ru

Линки на ресурсы

Инфо

Мы - представители русского хак-андеграунда, не потерпим провокации со стороны Грузии в любых ее проявлениях. Мы хотим жить в свободном мире, а существовать в свободном от агрессии и лжи Сетевом пространстве.

www.stopgeorgia.ru

Первоочередные цели для атак:

Сайт	Доступ с РФ (есть/нет)	Доступ с Литвы (есть/нет)
www.parliament.ge Парламент;	-	-
www.assistancegeorgia.org.ge Госкомстат;	+	+
www.cec.gov.ge Избирком;	+	+
www.mdf.org.ge Муниципальный фонд развития;	-	-
www.mfa.gov.ge МИД;	+	+
www.corruption.ge Anti-Corruption Program;	-	-
www.constcourt.gov.ge Конституционный суд;	+	+
www.constcourt.gov.ge Конституционный суд;	+	+
www.insurance.caucasus.net Страхование;	-	-
www.mc.gov.ge Минкультуры;	-	-
www.nsc.gov.ge Совет безопасности;	-	-
www.supremecourt.ge Верховный суд;	+	+
www.iberiapac.ge Минтранс;		
www.court.gov.ge Department of material service;	+	+
www.civil.ge Ассоциации ООН в Грузии;	-	-
http://georgia.usembassy.gov/ Посольство США в Тбилиси tbilisivisa@state.gov	+	+
http://ukingeorgia.fco.gov.uk/en Посольство ВБ в Тбилиси	+	+
http://www.all.ge/	-	-
http://www.geres.ge/	+	+
СМИ:		
www.rustavi2.com.ge Телеканал;	-	-
www.opentext.org.ge Электронные версии газет;	+	+
www.svobodnaya-gruzia.com Газета «Свободная Грузия»;	-	-
www.sanet.ge/gtze Газета Georgian Times;	-	-
www.messenger.com.ge Газета Georgian Messenger; http://georgianmessenger.blogspot.com/	+	+
www.primenewsonline.com Агентство «Прайм-ньюс»;	-	-
www.presidpress.gov.ge Информагентство	-	-
www.sakinform.ge	-	-
www.sakartvelo.ru	-	-
www.internews.ge	-	-
www.internews.org.ge	-	-
http://www.interpressnews.ge/	-	-
Другие		
http://www.internet.ge/	-	+
http://www.stream.ge/ - новости ТВ	-	+
http://newsgeorgia.ge/	-	-
http://presa.ge/	-	-
http://www.medianews.ge/	-	+

Новости

10.08.2008
Форум проекта запущен и работает в штатном режиме

09.08.2008
Отобран и опубликован список первостепенных целей для атак

09.08..2008
Открыт сайт, посвященный ведению информационной войны с Грузией

07.08.2008
Грузия развязала военный конфликт с Южной Осетией

Читать

[134] RBN – Georgia Cyberwarfare – Status and Attribution. Russia Business Network Exploit blog. rbnexploit.blogspot.com/2008_08_01_archive.html (last accessed: 30 Oct 2008)

Annex III: Chronology of Cyber Attacks against Georgia

Attack on the Georgian President website in July

On July 19, the website of Georgian President Mikheil Saakashvili (www.president.gov.ge) became unavailable for more than 24 hours due to a multi-pronged distributed denial of service (DDoS) attack. The Shadowserver Foundation observed at least one web-based command and control (C&C) server taking aim at the website, hitting it with a variety of simultaneous attacks. The C&C server instructed its bots to attack the website with TCP, ICMP, and HTTP floods. The website remained down for more than 24 hours and was later moved to a server in the US.

Commands picked up by Shadowserver[135]:

flood http www.president.gov.ge
flood tcp www.president.gov.ge
flood icmp www.president.gov.ge

Shadowserver also observed that HTTP-based botnet C&C server was a MachBot controller, which is a tool that is frequently used by Russian bot herders. The domain involved with this C&C server has seemingly bogus registration information but ties back to Russia. This server had recently come online in the past few weeks and had not issued any other attacks. All attacks observed were directed right at www.president.gov.ge.[136]

Shortly after the blog the C&C server that was used to issue these attacks was taken offline.

The attacks originally started to take place several weeks before the actual "intervention" with Georgian President's web site coming under DDoS attack executed by Russian hackers in July; followed by active discussions across the Russian web on whether or not DDoS attacks and web site defacements should in fact be taking place, because it would inevitably come as a handy tool to be used against Russia by Western or Pro-Western journalists. [137]

Georgian Cyber Attacks in August 2008

Shadowserver did not witness any other servers attacking Georgian websites from July 20 (when the blog was posted) until August 8, 2008. [138] A number of other sources also

[135] Adair, *supra* note 12.

[136] *Id.*

[137] Danchev, *supra* note 32.

[138] Adair, *supra* note 134.

confirm that the peak of DDoS attack and the actual defacements started taking place as of August 8. [139]

In the wake of the Russian-Georgian conflict (August 8), a week worth of speculations around Russian Internet forums materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with Georgia's Ministry of Foreign Affairs undertaking a desperate step in order to disseminate real-time information by moving to a Blogspot account. [140]

The date appears to coincide with military movement that has since escalated into fighting between the two countries. Since August 8 Shadowserver witnessed multiple C&C servers attacking websites that are Georgian or sympathetic to the country.[141]

Several Georgian state computer servers came under external control since shortly before Russia's armed intervention into the state commenced on August 8, leaving its online presence in disarray. While the official website of Mikheil Saakashvili, the Georgian President, has become available again, the central government site, as well as the homepages for the Ministry of Foreign Affairs and Ministry of Defence , remain down. Some commercial websites have also been hijacked. [142]

In a statement released via a replacement website built on Google's blog-hosting service, the Georgian Ministry of Foreign Affairs said on August 11, "A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs." [143]

After defacing Mikheil Saakashvili's web site and integrating a slideshow portraying Saakashvili as Hitler next to coming up with identical images of both Saakashvili and Hitler's public appearances, the site remains under a sustained DDoS attack (as of August 11). [144]

Nino Doijashvili (a Georgian expatriate), chief executive of Atlanta-based hosting company Tulip Systems Inc. offered the Georgian government help and transferred president.gov.ge and rustavi2.com, the Web site of a prominent Georgian TV station, to her company's servers on Saturday, August 9. [145]

---

[139] Danchev, *supra* note 29.

[140] *Id.*

[141] Adair, *supra* note 32.

[142] Danchev, *supra* note 29.

[143] 'Cyber Attacks Disable Georgian Websites', Georgian Ministry of Foreign Affairs, Aug 11, 2008, available at: georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html (last accessed: 27 Aug 2008).

[144] Danchev, *supra* note 29.

[145]Danchev, *supra* note 29.

On early morning of August 9, TBC, the largest commercial bank of Georgia came under attack.[146]

Dancho Danchev[147] of ZDNet monitored (presumably from Aug 9 to 10, 2008, as he referred to the weekend prior to posting his conclusions of Aug 11) the activities carried out in the course of the attacks and presented the following analysis, concluding the cyber attack was a coordinated one.[148] He made the following observations regarding the forms of attack employed in the timeframe:

Static lists of targets were distributed in order to eliminate centralised coordination of the attack.[149] A list of Georgian government web sites[150] was actively distributed across Russian web forums as targets to be attacked.[151] One such forum was stopgeorgia.ru (also redirect from stopgeorgia.info). [152]

DoS tools were provided, available for download from specific sites (Danchev understandably does not reference the sites, but does provide a screenshot) [153]. Instructions on **how to ping flood Georgian government web sites** were also distributed.[154]

Lists of Georgian sites vulnerable to defacement attack were published. Russian hackers started distributing lists of Georgian sites vulnerable to remote SQL injections, allowing them to automatically deface them.[155] As pointed out by the Project Grey Goose report, detection of a targeted SQL Injection attack designed to pilfer data or compromise the underlying system during a rigorous, traditional DDoS would be

---

[146] CERT-EE, *supra* note 26.

[147] Dancho Danchev is an independent security consultant and cyber threats analyst, with extensive experience in open source intelligence gathering, malware and E-crime incident response, and a security blogger since 2007, and maintains a popular security blog sharing real-time threats intelligence data with the rest of the community on a daily basis

[148] Danchev, *supra* note 29.

[149] *Id.*

[150] www.nbg.gov.ge

www.mof.ge

www.nsc.gov.ge

www.mod.gov.ge

www.constcourt.gov.ge

www.government.gov.ge

www.mfa.gov.ge

www.police.ge

[151] Danchev, *supra* note 29.

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Id.*

extremely difficult to detect, and the discovery and exploitation of these application level vulnerabilities shows both technical sophistication and planning, organization, targeted reconnaissance, and evolution of attacks.[156]

Abuse of public lists of email addresses of Georgian politicians for spamming and targeted attacks. The list was originally created by a lobbying organisation; during the attacks, it was circulated "in an attempt to convince Russian hackers of the potential for abusing it in spamming attacks and targeted attacks presumably serving malware through live exploit URLs". [157]

Attacking customary communication forums of the IT community: destroy the adversary's ability to communicate using the usual channels. One of Georgia's most popular hacking forums was under a long-lasting DDoS attack on behalf of Russian hackers who communicated the intent to ensure that local hacktivists could be reached.

On August 10, Shadowserver reported new attacks against .ge sites. (www.parliament.ge and president.gov.ge) were hit with http floods. In this case, the IP address of C&C server involved was 79.135.167.22 which is located in Turkey.[158]

This time, the attacks were not limited to just government websites. Shadowserver reported at least six different C&C servers attacking various websites that were not government sites. In some cases the servers were attacking the same websites. The following websites have come under attack:

www.president.gov.ge
www.parliament.ge
apsny.ge
news.ge
tbilisiweb.info
newsgeorgia.ru
os-inform.com
www.kasparov.ru
hacking.ge
mk.ru
newstula.info
skandaly.ru[159]

[156] Project Grey Goose, *supra* note 42

[157] Danchev, *supra* note 29.

[158] Adair, *supra* note 12.

[159] Adair, *supra* note 32.

By Aug 11**,** Civil.ge had come under DDoS attack, and — just like Georgia's Ministry of Foreign Affairs — it switched to a Blogger account in case the site remained unavailable.[160]

As of August 13, Shadowserver reported large-scale ICMP traffic. Attacks were directed against Georgian governmental websites from numerous Russian computers from several different ISPs throughout the country, covering both dialup and broadband users.[161] Russian blogs, forums, and websites are spreading a Microsoft Windows batch script that is designed to attack Georgian websites. The effect of it is continuous ICMP traffic via the 'ping' command to several Georgian websites.[162] Shadowserver also posted an example of the script[163] being posted:

```
@echo off
@echo Call this file (MSK) 18:00, 20:00
@echo Thanks for support of South Ossetia! Please, transfer this file to the friends!
pause
<removed> newsgeorgia.ru <removed>
<removed> apsny.ge <removed>
<removed> nukri.org <removed>
<removed> opentext.org.ge <removed>
<removed> messenger.com.ge <removed>
<removed> president.gov.ge <removed>
<removed> government.gov.ge <removed>
<removed> parliament.ge <removed>
<removed> nsc.gov.ge <removed>
<removed> constcourt.gov.ge <removed>
<removed> supremecourt.ge <removed>
<removed> cec.gov.ge <removed>
<removed> nbg.gov.ge <removed>
<removed> nplg.gov.ge <removed>
<removed> police.ge <removed>
<removed> mod.gov.ge <removed>
<removed> mes.gov.ge <removed>
<removed> mfa.gov.ge <removed>
<removed> iberiapac.ge <removed>
<removed> mof.ge <removed>
```

[160] Danchev, *supra* note 29.

[161] Adair, *supra* note 36.

[162] *Id.*

[163] Actual commands and parameters of the script have been removed to avoid being a distribution point for it.

According to Arbor Networks, a set of coordinated attacks followed the initial flood. These attacks were mostly TCP SYN floods with one TCP RST flood in the mix. No ICMP or UDP floods were detected; the attacks were all globally sourced, suggesting a botnet (or multiple botnets) were behind them.[164]

Number of attacks	Destination
5	213.131.44.138
3	213.157.196.25
10	213.157.198.33
1	www.gazeti.ge

Raw statistics of the attack traffic:

- Average peak bits per second per attack 211.66 Mbps
- Largest attack, peak bits per second 814.33 Mbps
- Average attack duration 2 hours 15 minutes
- Longest attack duration 6 hour[165]

The last large cyber attack against the Georgian websites was launched on August 27. After August 27, no serious attacks against Georgian cyberspace have been taken place, but nevertheless there have been occurrences of minor cyber attacks that are indistinguishable from regular traffic and can be attributed to regular civilians.

The main target of the August 27 attacks was the Georgian Ministry of Foreign Affairs that together with other sites came under a DDoS attack at approximately 16:18 (GMT +3). As the main target of the attacks was the Georgian Ministry of Foreign Affairs, the attacks mainly consisted of HTTP queries to the mfa.gov.ge website. These requests were generated to overload the web server in a way where every single request would need significant CPU time.

The cyber attacks also managed to disrupt services for other Georgian websites. This was so because of the load on the servers by these (HTTP) requests that resulted in rendering the services for the attacked websites slow and unresponsive.

The attacks started to wind down on August 28, due to the reason that most of the attackers were successfully blocked.[166]

---

[164] Nazario, *supra* note 33.

[165] *Id*.

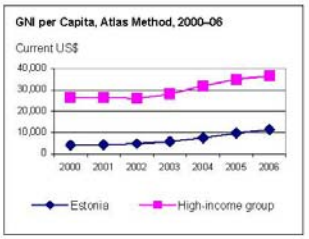
[166] Danchev, D. DDoS Attack Graphs from Russia vs Georgia's Cyberattacks. 15 Oct 2008. Available at: ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html (last accessed 25 Aug 2008).

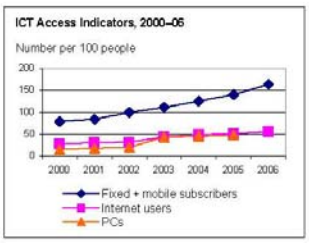
Annex IV: Estonian Information Society in Facts

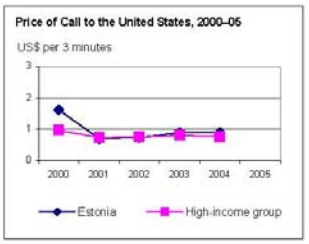
World Bank • ICT at a Glance

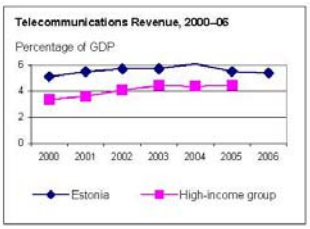
Estonia

	Estonia		High-income group
	2000	2006	2006
Economic and social context			
Population (millions)	1	1	1,031
Urban population (% of total)	69	69	78
GNI per capita, *World Bank Atlas* method ($)	4,120	11,400	36,608
GDP growth, 1995–2000 and 2000–06 (avg. annual %)	5.4	8.6	2.3
Adult literacy rate (% ages 15 and older)	100	..	*99*
Gross primary, secondary, tertiary school enrollment (%)	88	*92*	*92*
Sector structure			
Separate telecommunications regulator	Yes	Yes	
Status of main fixed-line telephone operator	*Mixed*	Mixed	
Level of competition (competition,partial comp.,monopoly)			
International long distance service	*M*	*C*	
Mobile telephone service	*C*	*P*	
Internet service	*C*	*C*	
Government prioritization of sector (1-7, 7=highest)	..	5.9	5.1
Sector performance			
Access			
Telephone mainlines (per 100 people)	38.2	40.4	52.7
International voice traffic (minutes per person)[a]	128	*109*	*204*
Mobile telephone subscribers (per 100 people)	40.7	123.6	90.1
Population covered by mobile telephony (%)	99	*99*	*99*
Internet users (per 100 people)	28.6	56.6	59.3
Personal computers (per 100 people)	16.1	*48.3*	*56.7*
Households with a television set (%)	91	*93*	*98*
Quality			
Telephone faults (per 100 mainlines)	19.2	..	*5.8*
Broadband subscribers (per 100 people)	*1.27*	17.00	19.20
International Internet bandwidth (bits per person)	137	11,175	*4,346*
Affordability			
Price basket for residential fixed line ($ a month)	9.4	*15.6*	*26.6*
Price basket for mobile telephone service ($ a month)	..	8.6	17.0
Price basket for Internet service ($ a month)	..	10.9	13.7
Price of call to United States ($ for 3 minutes)	1.62	*0.90*	*0.77*
Institutional efficiency and sustainability			
Telecommunications revenue (% of GDP)	5.1	5.4	*4.4*
Telephone subscribers per employee	354	*641*	*641*
Telecommunications investment (% of revenue)	17.6	*8.7*	*16.1*
Applications			
Sector expenditure (% of GDP)	..	..	7.2
E-government readiness index (0-1, 1=most ready)	..	0.76	0.74
Secure Internet servers (per million people, Dec. 2007)	*58.6*	215.5	569.4









Notes: Figures in italics are for years other than those specified. .. indicates data are not available. C = competition; GDP = gross domestic product; GNI = gross national income; ICT = information and communication technology; M = monopoly; MDG = Millennium Development Goal; P = partial competition; and PCs = personal computers.

a. Outgoing and incoming.

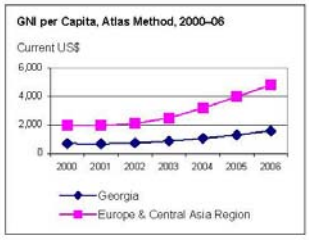
Sources. Economic and social context: UIS and World Bank; Sector structure: ITU, WEF; Sector performance: Global Insight/WITSA, ITU, Netcraft, UNDESA, UNPAN, and World Bank. Produced by the Global Information and Communication Technologies Department and the Development Economics Data Group. For complete information, see Definitions and Data Sources.

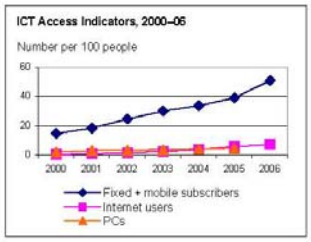
Annex V: Georgian Information Society in Facts

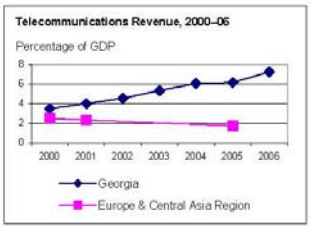
World Bank • ICT at a Glance

Georgia

	Georgia		Lower-middle-income group	Europe & Central Asia Region
	2000	2006	2006	2006
Economic and social context				
Population (millions)	5	4	2,276	461
Urban population (% of total)	53	52	47	64
GNI per capita, *World Bank Atlas* method ($)	700	1,580	2,038	4,815
GDP growth, 1995–2000 and 2000–06 (avg. annual %)	5.7	7.8	7.6	5.8
Adult literacy rate (% ages 15 and older)	..	..	*89*	*97*
Gross primary, secondary, tertiary school enrollment (%)	74	*76*	*71*	*82*
Sector structure				
Separate telecommunications regulator	Yes	Yes		
Status of main fixed-line telephone operator	..	..		
Level of competition (competition,partial comp.,monopoly)				
International long distance service	*P*	*C*		
Mobile telephone service	*C*	*C*		
Internet service	*C*	*C*		
Government prioritization of sector (1-7, 7=highest)	..	3.8	4.3	4.4
Sector performance				
Access				
Telephone mainlines (per 100 people)	10.8	12.5	21.6	*24.6*
International voice traffic (minutes per person)[a]	29	*58*	*21*	..
Mobile telephone subscribers (per 100 people)	4.1	38.4	38.1	*63.5*
Population covered by mobile telephony (%)	*79*	96	..	..
Internet users (per 100 people)	0.5	7.5	11.4	19.2
Personal computers (per 100 people)	2.4	*4.7*	*4.3*	*10.2*
Households with a television set (%)	81	*89*	*80*	*97*
Quality				
Telephone faults (per 100 mainlines)	26.3	..	*22.0*	*9.5*
Broadband subscribers (per 100 people)	*0.01*	0.61	3.23	3.64
International Internet bandwidth (bits per person)	*2*	*7*	189	*268*
Affordability				
Price basket for residential fixed line ($ a month)	4.2	*9.7*	*8.2*	*7.2*
Price basket for mobile telephone service ($ a month)	..	44.1	9.8	11.8
Price basket for Internet service ($ a month)	..	*9.9*	10.0	11.1
Price of call to United States ($ for 3 minutes)	2.88	..	*2.08*	*1.55*
Institutional efficiency and sustainability				
Telecommunications revenue (% of GDP)	3.5	7.3	*2.1*	*1.7*
Telephone subscribers per employee	69	*197*	*599*	*314*
Telecommunications investment (% of revenue)	*65.4*	*30.9*	*27.1*	*22.0*
Applications				
Sector expenditure (% of GDP)	..	..	5.0	4.6
E-government readiness index (0-1, 1=most ready)	..	0.46	0.45	0.49
Secure Internet servers (per million people, Dec. 2007)	*2.1*	7.7	1.6	17.3







Notes: Figures in italics are for years other than those specified. .. indicates data are not available. C = competition; GDP = gross domestic product; GNI = gross national income; ICT = information and communication technology; M = monopoly; MDG = Millennium Development Goal; P = partial competition; and PCs = personal computers.

a. Outgoing and incoming.

Sources: Economic and social context: UIS and World Bank; Sector structure: ITU, WEF; Sector performance: Global Insight/WITSA, ITU, Netcraft, UNDESA, UNPAN, and World Bank. Produced by the Global Information and Communication Technologies Department and the Development Economics Data Group. For complete information, see Definitions and Data Sources.

Annex VI: Comparison of Recent Cyber Conflicts

	Estonia 2007	Lithuania 2008	Georgia 2008
Background	Political events: relocating a Soviet war memorial.	Political events: On June 17 2008, Lithuanian Parliament passed a law prohibiting the public display of symbols dating from the Soviet Union era, as well as playing of the Soviet Union anthem.	Georgian surprise attack against separatist forces in South Ossetia resulted in Russian aggression. Cyber attacks against Georgia occurred simultaneously with physical attacks.
Duration	27 April - 18 May, 2007	28 June – 30 June, 2008	July 19-20, August 7-27, 2008
Targets	Political, Services (On-line banking, ISPs, Online media); Personal and random targets.	Political and private sites (all hosted on the same ISP).	Political (Governmental and presidental sites), Services (Online banking, Online media, ISPs) .
Damages	Unestimated	Unestimated	Unestimated
Attack types	DoS and DDoS, defacement, e-mail and comment spam, Some targeted hacks using exploits/SQL injections.	Defacement.	DoS and DDoS, defacement, TCP SYN floods, TCP RST flood, Higher intensity attacks compared to Estonia 2007.
Attackers	Unknown. Attacks globally sourced. Using (paid) botnets and random internet users. Instructions widely available on the Internet.	Unknown. Attacks conducted via proxy servers. Controversial information about the location of the servers – some sources indicate that attacks originated	Unknown. Attacks globally sourced. Using (paid) botnets and random internet users. Instructions widely available on the Internet.

		from the servers located outside Lithuania, while others point that the servers were located in the east territories of Lithuania.	
Defensive and organisational actions	Cooperation (CERT-EE + network of specialists, international cooperation). Political coverage. Media coverage. Law enforcement actions. Technical countermeasures.	Cooperation (CERT-LT, Academic and Research Network CERT). Political coverage. Media coverage. Technical countermeasures. Police investigation.	Cooperation (Georgian University CERT, CERT-EE, CERT-PL, CERT-FR). Political coverage. Media coverage. Technical countermeasures.