DEVELOPMENTS IN THE LEGISLATIVE, POLICY AND ORGANISATIONAL LANDSCAPES IN ESTONIA SINCE 2007

Kadri Kaska[58], Anna-Maria Talihärm[59], Eneken Tikk[60]

Abstract

In April and May 2007, Estonia faced coordinated cyber attacks targeted at the Estonian governmental and commercial entities. The attacks drew strong attention to the need to raise international awareness about politically motivated and coordinated cyber attacks directed against a nation state and, more generally, against the modern information societies that are increasingly dependent on information technology. Three years after the attacks, it is increasingly evident that cross-border cyber incidents such as Estonia 2007 touch upon legal norms of different legal fields and therefore need to be viewed from the three-fold prism of Law of Armed Conflict, Criminal Law, and IT legal framework, thus supporting the comprehensive approach to the domain. This article examines the developments in the area of cyber security in Estonia and in what ways the Estonian legislation, policy approaches as well as organisational landscape have evolved since April 2007.

INTRODUCTION

The level of dependency on information technology and differences in approaches, in motivation of interest groups as well as principles employed in regulating information societies vary greatly from nation to nation. This combined with the rapid progress of information technology often complicates the practical implementation of legislative measures necessary to ensure cyber security at the national and, moreover, at the international level.

58 Kadri Kaska is a Junior Scientist of the NATO-accredited Cooperative Cyber Defence Centre of Excellence.
59 Anna-Maria Talihärm is a Junior Scientist of the NATO-accredited Cooperative Cyber Defence Centre of Excellence and a PhD student of Tartu University Faculty of Law.
60 Eneken Tikk is a Scientist and the Head of the Legal Team of the NATO-accredited Cooperative Cyber Defence Centre of Excellence. She was a Research Fellow of GMU CIP and is a PhD student of Tartu University Faculty of Law.

Similarly, the expanding divide between the views of legal scholars in the field of cyber defence law produces numerous valuable theories, doctrines and guidance without having too much regard to counterarguments and assessments of the practical impact from policy and technological perspective. This, in return, brings about the unfortunate effect of a colourful abundance of articles, books, conferences on the subject and a number of think tanks dealing with cyber issues, while at the same time players involved in real-life cyber incidents have access only to a handful of practical solutions.

Much has been written on the legal aspects of cyber security and defence, and most of these discussions can be divided into three main research areas: Law of Armed Conflict (LOAC), Criminal Law, and practical IT Law. However, much of this research has been stove-piped, i.e. focused on the specific area of expertise and individual security planning instead of a coordinated and interdisciplinary approach.

There are multiple reasons why legal research in the cyber security/defence area has developed in such isolated manner, two of them being the most relevant. First, for a long time cyber defence has been a "closed circuit" responsibility and domain of individual corporations, governments, organisations and working groups. This has led to a situation where numerous think tanks exist in the field but no general agreement seems to prevail that would include practical input for those who have to respond to contemporary cyber incidents.

The second reason – which very much derives from the first one – is that the wide spectrum of cyber threats has not been visible to all subject matter experts at the same time in the same manner. While the military domain has dealt mainly with information operations (IO)[61] and electronic warfare (EW)[62], criminal law experts have been busy with identity theft and credit card fraud[63], and IT legal experts have been working on developing legal policies that would harmonise the security concerns of the private sector with public and national interests[64].

In this context it is understandable how various players such as nations and organisations have ended up with different views on the domain of cyber security. Different perspectives, however, should not prevent nations from critically reviewing their regulation in the context of new emerging threats and

61 Information Operations, Joint Publication 3-13, Joint Chiefs of Staff, US Army, 2006, available at: http://www.fas.org/irp/doddir/dod/jp3_13.pdf.
62 Electronic Warfare, Joint Publication 3-13.1, Joint Chiefs of Staff, US Army, 2006, available at: http://www.fas.org/irp/doddir/dod/jp3-13-1.pdf.
63 Online Identity Theft, OECD, Directorate for Science, Technology and Industry, 2009, available at: http://www.oecd.org/document/44/0,3343,en_2649_34223_42420716_1_1_1_1,00.html.
64 Strategies for Cybersecurity and Critical Information Infrastructure Protection, ITU, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html.

implementing a comprehensive approach to cyber security by involving a wide range of stakeholders, coordinated decision-making and multiple areas of regulation.

The aim of this article is to follow closely the development of cyber security framework by examining the legal aftermath of the Estonia 2007 cyber attacks. The article argues that a practical and viable approach to cyber security and defence – one that is able to offer a comprehensive set of effective measures for preparedness, response and mitigation – includes all of the above-mentioned fields of law.[65]

Thereby, the article will use the Estonia 2007 case study to demonstrate, with the benefit of a 3-year retrospective, the legal, policy and organisational lessons learned from a cyber incident. Based on the assumption that the changes undergone reflect weaknesses in the legal system identified by the attacks, we may presume that these were the areas of information society regulation where the need for amendments was most clear. The study also suggests that the first steps for a nation that aims for a better coordination in the domain of cyber security would be defining relevant terminology, reviewing the legislative system, and enforcing effective application of the cyber security strategy.

Different Perspectives on Cyber Security

Cyber incidents such as Georgia 2008[66], Lithuania 2008, Radio Free Europe/Radio Liberty 2008 have reinforced the understanding that conflicting points of view often tend to arise from different background systems[67] and experiences that do not support the same or even similar legal conclusions.[68] Consequently, the ability to consider the different relevant sides of the story and the ability to systematically categorise the different types of cyber activities has enormous significance from the legal perspective. Under the rule of law and especially the principle of *nullum*

65 This approach can also be called Frameworks for International Cyber Security (FICS). Read more, Tikk, Eneken, Frameworks for International Cyber Security. CCD COE Publishing, 2010.

66 The Georgian incident especially illustrated the need to look to the criteria of applicability of different legal regimes and the remedies available therein. Both are addressed in Tikk, Eneken; Kaska, Kadri; Vihul, Liis, International Cyber Incidents: Legal Considerations, CCD COE, 2010, See pp. 25-26 for Estonia and pp. 79-88 for Georgia.

67 While international law and law of armed conflict tend to be what many practicing attorneys would call "too abstract for a good argument", IT legal issues are very practical and often do not have a long legal history behind them. It is therefore seldom that lawyers have to practice both of these disciplines.

68 For a more complete fact description and legal analysis, see Tikk, Eneken; Kaska, Kadri; Vihul, Liis. International Cyber Incidents: Legal Considerations. CCD COE, 2010.

crimen nulla poena sine lege[69] known to criminal law, it may be highly complicated to draw any legal consequences from an act that cannot be clearly related to an existing legal regime or framework. From a practical point of view, therefore, a clear understanding of "what is what" in terms of applying the corresponding legal regime is of crucial importance.[70]

Side by side with the necessity of taking into account the various national approaches to cyber security it is vital to integrate these different perspectives in order to define a common point of departure for managing cyber security incidents. As explained above, a segmented approach often continues to prevail within law related to national cyber security. The historic segmentation of different fields of law has caused employing a similar segmented approach in the domain of cyber security regulation. While there are examples of countries that have adopted or are currently preparing or considering cyber security "umbrella acts"[71] intending to address a number of cyber security related legal issues within one law, it is also true that none of those cases truly involve all areas of law relevant to cyber security. Rather, they are often aimed at achieving particular cyber security objectives, address diverse national cyber security problems, and originate from very different reasons, which is why it is difficult to derive a regulatory model based on these examples.

There are arguments that speak for an all-inclusive cyber security regulation – re-structuring the current system of a number of ministries and public institutions all sharing the competence over cyber security under one overseeing body would better coordinate national initiatives, cut back on duplicated effort and waste of resources, as well as result in a more effective overall defence. However, a comprehensive approach does not necessarily mean that all cyber-related matters of different fields should be brought under a common legal framework and/or a common managing body. In fact, there are sound arguments to indicate that the

69 The principle of '*nullum crimen, nulla poena sine lege*' originates from continental European legal systems and has nowadays become a fundamental right which is enshrined in several national constitutions and a number of international instruments. In Estonian legislation, the principle is stated in the Estonian Penal Code (§ § 2 and 5). The n*ullum crimen, nulla poena sine lege* principle is a legal principle that prohibits retrospective criminalisation of acts and omissions. The principle states that no person may be punished for an act that was not a criminal offence at the time of its commission and results in the prohibition of applying law by analogy and requirement of specification of an offence.

70 The issue of how to categorise information warfare attacks is of more than academic interest. First, whether or not an information warfare attack can be considered an act of "war", "force" or „aggression" is relevant to whether a particular response would be proportionate to the original attack. See Greenberg, Lawrence T. and others, Information Warfare and International Law, 1998, page 19.

71 E.g. the U.S.A. (Protecting Cyberspace as a National Asset Act 2010), India (Information Technology Act 2000), Latvia (Cyber Security Framework Act, draft as of summer 2010), and Slovakia (the drafting of a uniform legal act was discussed in the spring of 2010).

reverse may be advisable.

One of them lies in the evolvement of regulating information technology. Since cyber is not a "thing in itself" but a merely a means to support the functioning of state and society, law of information technology has developed under the same concept of regulation supporting certain societal functions on a sectoral basis. It may be unreasonably resource-consuming, if not entirely unrealistic, to reshape the legal systems from a function-based to a tool-based approach. This function-based approach is also reflected in the current setup of and task division between national administrations, where a balance is needed to ensure that one agenda does not unduly dominate over another, equally justified one (e.g. security over economic growth and welfare or *vice versa*).

However, a comprehensive approach does mean that there should be a greater degree of involvement of different bodies shaping and affecting policy in cyber related matters, and a greater level of cooperation between them, which is where national cyber security strategy drafting might come in as a useful forum.

Overview Of The Estonia 2007 Incident

In the spring of 2007, Estonia suffered from an unprecedented amount of coordinated cyber attacks against its private and public institutions. The attacks – mainly denial of service (DoS) and distributed denial of service (DDoS) attacks – were triggered by the relocation of a Soviet World War II war memorial and targeted at the Estonian governmental agencies, banks, as well as media channels and private web sites. At the their peak, the amount of data traffic originating from the outside of Estonia and targeting governmental institutions was hundreds of times higher than its normal rate.[72] While the intensity of attacks or the choice of targets was not completely unprecedented, the extent, amount and duration of the attacks combined and the manner of coordination employed was not comparable to anything that a single nation state had experienced, and the sequence of attacks quickly gained attention worldwide.

Estonia has over the years become an example of an effective e-state[73] where an impressive choice of public e-services and databases – governmental as well as commercial – has been integrated into a nation-wide information system accessible throughout the country. The high level of IT development reveals an increasing dependence on e-services and the Internet as well as explains the vulnerability of

72 Tikk, Eneken, Oorn, Reet, Legal and Policy Evaluation: International Coordination of Prosecution of Cyber Terrorism, 2007.

73 A few examples: Estonia was the first country to hold Parliamentary elections online in 2005 and 95% of Estonia's banking operations are carried out electronically.

the country to a wide range of cyber offences. This dependency and vulnerability is characteristic to all modern information societies.

The attacks started on April 27 and disrupted Estonian e-services and information infrastructure in several waves of varying intensity until the end of May. Roughly, two phases could be distinguished in the incident: an initial emotional cyber response to the government's political decision of relocation of the monument (which ran in parallel to riots on the streets of the country's capital) was soon followed by more sophisticated and coordinated cyber assaults. The first phase lasted for a few days and was characterised by relatively simple DoS attacks against government web servers and Estonian news portals. The attacks did not appear to be centrally coordinated and were carried out mostly on *ad hoc* basis, boosted by online step-by-step instructions with a pre-defined list of targets.[74]

The second phase was characterised by the use of larger botnets and more sophistication[75] with the attacks involving more than 85,000 hijacked computers.[76] The abrupt waves of attacks[77] referred to better coordination; also a clear correlation was noticeable between the politically significant dates and intensification of the attacks.[78] Similarly to the first phase, Internet forums and chat rooms were used to distribute instructions and information about launching the "do-it-yourself" attacks but most of the attacks launched during the second phase appeared to be better and more systematically coordinated.

Some of the DDoS attacks were temporarily successful and managed to disable the online services of two biggest banks in Estonia and at one point shut down 58 websites[79] at the same time. Additionally, various attacks were performed against critical routers at Internet service provider level, which disrupted the government's Internet based communication for a short period of time. On top of that, both of the phases included website defacement and large amounts of email and comment spam.

Even though from a conservative lawyer's point of view, the Estonian 2007 cyber attacks did not amount to more than a series of cyber crimes, the media quickly

74 Evron, Gadi, Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War, Georgetown Journal of International Affairs, Winter/Spring 2008, p 121-126.
75 Nazario, Jose. Estonian DDoS Attacks - A summary to date, 17.05.2007. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.
76 Tikk, Eneken; Kaska, Kadri; Vihul, Liis. International Cyber Incidents: Legal Considerations. CCD COE, 2010, p. 20.
77 Graphs about the Estonian cyber attacks 2007, available at: http://www.riso.ee/wiki/Riots.
78 Tikk, Kaska, Vihul, Legal Considerations, p 18.
79 Nazario, Jose. Estonian DDoS Attacks - A summary to date, 17.05.2007. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

labelled the attacks "Cyber War I".[80] Security analysts argued that in comparison to other DoS and DDoS attacks[81], the size of the Estonian attacks was not groundbreaking.[82] Similarly, the Estonian government concluded in June 2007 that the cyber-attacks carried out against Estonia in April and May did not paralyse the country's normal daily activities, although, under certain conditions, could have posed a significant security risk.[83] On the international level, it was the element of political and social motivation that rendered the attacks globally noteworthy.

Since attribution is one of the crucial elements in solving any cyber incident, the identification of the attacker received significant attention both on national and international communities. There still prevails a popular belief that the large-scale cyber attacks against the Estonian government's servers and critical private information infrastructure in 2007 were initiated by and carried out from Russia. However, Konstantin Goloskokov, a member of a pro-Kremlin youth association *Nashi*, has been so far the only person publically admitting[84] taking part of the cyber attacks stating that "cyber attacks against Estonia seemed to be the only possible step."[85] Despite speculations on the political level[86], the exact origin of the attacks has not been confirmed in legally waterproof terms. What can be deducted from available facts is that a part of the attacks was carried out voluntarily by regular citizens and Internet users following instructions and sharing experiences on web forums (albeit mostly Russian)[87], and that the attacks were dispersed worldwide involving computers from 178 countries[88]. Nonetheless, any government's explicit role in the attacks cannot be confirmed.

Technical Measures Of Response

In the 2007 cyber attacks, the Computer Emergency Response Team of Estonia

80 Landler, Mark; Markoff, John. 'In Estonia, what may be the first war in cyberspace.' International Herald Tribune. 28 May 2007. http://www.iht.com/articles/2007/05/28/business/cyberwar.php.
81 Vamosi, Robert, Cyberattack in Estonia--what it really means, ZDNet, available at: http://www.zdnet.com/news/cyberattack-in-estonia-what-it-really-means/152212.
82 *Nazario, Jose, Estonian DDoS Attacks – A summary to date, Arbor Networks, available at: http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.*
83 Cabinet Approves Action Plan to Fight Cyber-attacks. http://www.ria.ee/index.php?id=28731.
84 Estonia has so far convicted only one 20-year-old hacker. Dmitri Galushkevich used his home computer to bring down Reform Party's website. Read more e.g. Sachoff, Mike, Man Convicted In Estonia Cyber Attack, WebProNews, 24.01.2008. http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack (25.05.2008).
85 Mõttus, Kristiina, Naši komissar: küberrünnak Eesti vastu näis ainuõige sammuna. http://www.postimees.ee/290507/esileht/siseuudised/263405.php.
86 See e.g. Rand, Erki, Laar: suutlikkus Venemaa küberrünnakud tõrjuda on tõstnud Eesti mainet, Eesti Päevaleht, 11.07.2007. http://www.epl.ee/artikkel/392744.
87 Evron, Gadi; Aarelaid, Hillar. Estonia: Information Warfare and Lessons Learned. [2007] Available at: http://ec.europa.eu/information_society/policy/nis/docs/largescaleattacksdocs/s5_gadi_evron.pdf .
88 Kremlin-backed group behind Estonia cyber blitz. http://balticbusinessnews.com/Print.aspx?PublicationId=b737410e-e519-4a36-885f-85b183cc3478.

(CERT-EE) became the coordinating body for response to the attacks, engaging local service providers and a network of IT professionals on a voluntary basis from both the governmental and commercial sector, and experts both within and outside of the country.[89] The CERT's emergency response program involved analysing the severity of the incident, sending abuse reports to service providers abroad, and facilitating information exchange between the affected organisations and service providers.[90] Some assistance, primarily in the form of consultation, was also received from international organisations such as NATO.

It was however noted that even though the Estonian CERT was able, to a degree, to mitigate the impact of the attacks, due to the *ad hoc*, unofficial status of its tasking, it lacked the authority to enforce its recommendations on all parties involved.[91]

Regardless of the malicious attacks against Estonian web pages, Estonia tried to keep up domestic Internet traffic and visits to foreign web pages were mostly possible. Whilst most public sector web pages were accessible to domestic users, restrictions applied to Internet users abroad.[92]

THE LEGAL, POLICY AND ORGANISATIONAL RESPONSE: POST-2007 DEVELOPMENTS IN THE FIELD OF CYBER SECURITY

The 2007 attacks triggered modifications in the Estonian legislative situation and institutional landscape or in some cases supported or enhanced the changes already under way. Some of these changes were materialised over the period of 2007-2010, some still continue to be implemented.

The cornerstone of the recent developments is the national Cyber Security Strategy, adopted in May 2008.[93] In order to achieve the goals set in the strategy, a set of implementation documents has been approved that foresee a number of concrete measurable actions within the high priority areas of critical information infrastructure protection, overall competence of information security, relevant legal framework, international cooperation and awareness of cyber security issues.

89 Tiks, Oliver. 'Küberrünnakuid tõrjuvad sajad spetsialistid' (In Estonian). Postimees Online, 2 May 2007. Available at http://www.tarbija24.ee/120507/esileht/siseuudised/258274.php.
90 Evron, Gadi. 'Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War'. *Georgetown Journal of International Affairs,* Winter/Spring 2008, p 123.
91 *Ibid.*
92 'Malicious cyber attacks against Estonia come from abroad'. Press release by the Estonian Informatics Centre, http://www.ria.ee/index.php?id=28623.
93 For a more detailed introduction into the Estonian Cyber Security Strategy, see section 5.3.1 of this paper.

The strategy identified three legal fields in need of immediate review and updating: the legal regulation for tackling cyber crime, supporting the availability of CIIP, and indicating information security standards for critical information systems. Deriving from there, the main legislative changes encompassed two major legal acts: the Penal Code, where both substantive and procedural law amendments were adopted by the Parliament in March 2008, and the new Emergency Act (adopted in 2009), which now accommodates threats to critical information infrastructure.

In 2010, the Estonian Informatics Centre (EIC), a central government body responsible for government information systems as well as the Estonian national CERT, was supplemented by a new entity: Department for Critical Information Infrastructure Protection (CIIP)[94]. The tasks of the new department include creating a defence system for Estonia's critical information infrastructure and the protection of important IT systems of the public and private sectors alike. In May 2010, the government announced its intention to upgrade the Estonian Informatics Centre into a national cyber security organisation with full a mandate to exercise regulatory powers.[95]

The main developments in the fields of law, policy and organisational structure that were undergone after the 2007 attacks are discussed in more detail below.

CYBER SECURITY RELATED AMENDMENTS IN THE ESTONIAN LEGAL FRAMEWORK

Penal Code

In the aftermath of the 2007 cyber attacks, the terminology, elements and definitions of cyber crime in the Penal Code were thoroughly revised by several amendments. The reasons for the revision originated mostly in the need to harmonise the Estonian Penal Code with the Council of Europe Convention on Cybercrime[96] and the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[97], and to update the definition of "Acts of terrorism" (§ 237 of the Penal Code) in order to ensure its comprehensiveness and applicability to the cyber domain.

94 Kriitilise informatsiooni infrastruktuuri kaitse osakond (KIIK).
95 Infosüsteemide arenduskeskus saab võimu juurde, Postimees online, available at: http://www.postimees.ee/?id=262349.
96 http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.
97 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systemshttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT.

Taking into account the complications that arose in the prosecution of the 2007 spring cyber attacks, the Ministry of Justice prepared a comprehensive amendment package to the Penal Code which was presented to the *Riigikogu* (Estonian Parliament) in December 2007 and adopted as law in February 2008.[98]

The amendments itemised in more detail the provisions of the Penal Code relating to attacks against computer systems and data, updated the extent of some provisions (such as adding the dissemination of spyware and malware) and added a new provision on preparation of cyber crimes. Based on the understanding that the frequency of cyber attacks has been on a steady rise, and that due to the rising availability of Internet and growing use of electronic channels by the population such attacks are becoming increasingly dangerous, the amendments also prescribed higher maximum punishments and corporate liability for such crimes.

Crimes against Computer Data and Computer Systems

The amendments[99] approved in 2008 followed the wording and structure of the Convention on Cybercrime by clearly distinguishing the two clauses § 206 "Interference in computer data" and § 207 "Hindering the operation of computer system" which previously had been combined in one paragraph. The text of the provisions as amended now stands:

§ 206 "Interference in computer data"

Illegal alteration, deletion, damaging or blocking of data or programmes within computer systems, or illegal uploading of data or programmes into computer systems is punishable by a pecuniary punishment or up to three years of imprisonment.

§ 207 "Hindering the operation of computer system"

Illegal interference with or hindering of the operation of a computer system by way of uploading, transmitting, deleting, damaging, altering or blocking of data is punishable by a pecuniary punishment or up to three years of imprisonment.

Whereas § 206 does not require any damage to be caused to qualify as "Interference in computer data", acts criminalised under § 207 need to involve an actual hindrance of and subsequent damage to a computer system. Similarly

98 The last available English translation of the Estonian Penal Code dates back to April 2008 and is available at the website of the Estonian Ministry of Justice at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik.

99 Karistusseadustiku muutmise seaduse eelnõu 166 SE II-1. http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20100318225035&file_id=256023&file_name=166s-XI.doc&file_sise=32256&mnsent=166+SE&fd=01.12.2009 (in Estonian).

to the Convention, § 207 outlines the possible ways of hindering the operation of a computer system, including damaging, deletion, deterioration, alteration or suppression of computer data without right. Thus, the new wording clarifies the possible elements of the crime and covers such acts as DoS, DDoS, and spamming. The paragraph also prevents qualifying any type of interference such as physical damaging or destruction of the computer systems or cables under § 207.

Additionally, the amendments resulted in increasing the level of punishment for certain acts under § 206, § 207, § 217, namely for attacks aimed against the computer systems of critical infrastructure. Critical infrastructure is defined and the objects of critical infrastructures listed in the Emergency Act (see section 5.2.3 of this paper).

Article 6 of the Cyber Crime Convention that regulates the misuse of computer devices was, prior to 2007, essentially uncovered by the Estonian Penal Code. After the adoption of the 2008 amendments, the new § 216[1] "Preparation of computer-related crime" asserts criminal responsibility for preparatory acts that are intended to be used for the purpose of committing any of the offences established in § 206, 207, 208, 213 or 217 of the Penal Code. These include the production, owning, distribution or otherwise making available of equipment, programs, codes or other data for accessing a computer system and using, distribution or otherwise making available of data necessary for committing the abovementioned crimes.

Computer Virus, Malware and Spyware

The aim of Article 4 in the Convention on Cybercrime is to provide computer data, computer programs and systems with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The input of malicious code, such as viruses, Trojan horses, malware and spyware is, therefore, covered under the Convention Article 4 "Data interference" as the acts result in the modification of data.[100]

§ 208 in the Estonian Penal Code originally exclusively addressed dissemination of computer viruses. The provision was later extended to include malware and spyware. The difference compared with § 206 "Interference in computer data" lies within the fact that using malicious code, viruses, malware, spyware and the kind does not imply the actor's active interference in the data of a computer system. The actor does not physically alter the data; rather, it is done by the malicious program.

It is interesting to note that § 208 regulates only the dissemination of computer

100 See the Explanatory Report to the Council of Europe Convention on Cybercrime. http://conventions.coe.int/treaty/en/reports/html/185.htm.

virus, malware and spyware, whereas § 216[1] criminalises the preparation of such programs.

Similarly to the previously mentioned clauses, the new wording of § 208 involves more severe sanctions for computer-related crime. Committing an act qualifiable as § 208 is punishable by pecuniary punishment or up to 3 years' imprisonment (compared to the 1-year imprisonment foreseen previously). If the same act is committed repeatedly, i.e. at least for the second time, or causes significant damage, the punishment can be a pecuniary punishment or up to 5 years' imprisonment.

Acts of Terrorism

Under the law prior to the 2007 attacks, Penal Code § 237 "Acts of terrorism"[101] read as follows:

> *Commission of a criminal offence against international security, against the person or against the environment, or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population is punishable by five to twenty years' imprisonment, or life imprisonment.*

In 2008, the § 237 of the Penal Code was amended to include "interference with computer data or hindrance of operation of computer systems as well as threatening with such acts'.[102] According to the new wording, an act of cyber crime, if motivated by terrorist aims and fulfilling the elements listed above, should be treated as terrorist crime by the Estonian law.[103]

The amended § 237 filled an important gap in the Penal Code by enabling differentiation between cyber attacks against critical infrastructure (with the purpose of seriously interfering with or destroying the economic or social structure

101 See also Explanatory note on the amendment of Penal Code. http://www.riigikogu.ee/?page=pub_ooc_file&op=emsplain&content_type=text/html&file_id=198499.
102 Estonian Penal Code (RT I 2001, 61, 364; 2009, 39, 261), § 237.
103 Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code (116 SE). (In Estonian.) December 2007. Available at: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20090902161440&file_id=198499&file_name=KarS%20seletuskiri%20(167).doc&file_size=66048&mnsensk=166+SE&etapp=03.12.2007&fd=29.10.2008.

of the state) and ordinary computer crime. A cyber attack against a country can disturb the functioning of the public authority or the provision of public services and it is therefore necessary to guarantee additional protection deriving from the criminal law. The provision also covers those possible cases of cyber terrorism where politically or socially motivated serious attacks against data or computer systems may result in severe economic loss or bloodshed.

Amendments Relevant to Procedural Law

The above-mentioned amendments in the Penal Code were partly brought about by the legal limitations that arose from the application of criminal procedure law[104] in co-effect with the Estonian Surveillance Act.[105]

As the investigation and identification of the originators of the attacks is always dependent on legally permissible measures, one of the founding applicable legal acts in the investigational matters is the Estonian Surveillance Act. According to the act, collecting information concerning data communicated via electronic communications networks is permitted only to surveillance agencies within the limits of their competence and within procedures authorised by law.[106] Thus, unauthorised surveillance, for example the unauthorised observing of a person's activities in order to collect information relating to that person, is criminalised and punishable by law.[107] According to the Act, monitoring and analysing data logs with the objective of identifying particular attackers does not belong to the competence of ISPs or CERT-EE and is reserved to law enforcement agencies.

§§ 110-112 of the Code of Criminal Procedure state that evidence may be collected by surveillance activities in a criminal proceeding if the collection of evidence by other procedural acts is a) precluded or especially complicated and b) the criminal offence under investigation is, at the minimum, an intentionally committed crime for which the law prescribes a punishment of at least three years' imprisonment.[108] Still, almost none of the criminal acts committed during the Estonian cyber attacks managed to meet the 'three years' imprisonment as punishment'-level.

104 Code of Criminal Procedure (RT I 2003, 27, 166; 2010, 40, 239). An unofficial English translation is available at http://www.legaltext.ee/text/en/X60027K6.htm.
105 RT I 1994, 16, 290; 2009, 62, 405. An unofficial English translation is available at http://www.legaltext.ee/text/en/X30011K7.htm
106 These are the Security Police Board, Police and Border Guard Board, the Military Police, the Prisons Department of the Ministry of Justice and prisons, and the Tax and Customs Board. *See* § 12 (1) section 5, § 6 (1) and (2) of the Estonian Surveillance Act.
107 § 137 of the Estonian Penal Code. Penal Code of Estonia (RT I 2001, 61, 364; 2009, 39, 261). An unofficial English text is available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik.
108 § 110, 117 of the Estonian Code of Criminal Procedure.

The punishment prescribed by the 2007 Penal Code was pecuniary punishment or a maximum one year of imprisonment[109] and that disabled the applicability of surveillance activities.

Since collecting of evidence is complicated in investigating such crimes, the Penal Code amendments concerning the extension of the term of punishment for computer-related crimes to up to three years, made the use of surveillance measures available for the police.[110]

New Emergency Act

A part of the response to improve national resilience to cyber threats was the new Emergency Act[111] adopted in June 2009. For the purpose of drafting the new Act, an inter-ministerial working group was set up under the lead of the Ministry of the Interior in the spring of 2008, tasked with identifying critical infrastructure – including critical information infrastructure – and reviewing and updating the current setup of emergency preparedness in Estonia. Cyber security experts from different government agencies were involved in the project from the beginning.

The purpose of this undertaking, however, was wider than merely addressing cyber threats. Rather than following a segmented approach, the act was to comprehensively address all national emergency situations, laying a foundation for a uniform organisational emergency handling structure and procedural framework for emergency response. National *cyber security* threats were thus included under the general framework set up by the act; certain provisions also specifically address threats against information systems.

The act regards as 'emergency' those events which endanger, on a significant scale, the life or health of people, or cause significant proprietary or environmental damage, or cause severe and extensive disruptions in the continuous operation of vital services, and require prompt coordinated activities of several agencies in response. The definition is effect-based (the criteria being death and injury of people or destruction of property) rather than source-based – it does not differentiate whether the effect was caused by human, technological or natural

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

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

111 RT I 2009, 39, 262; 2010, 24, 115. An unofficial English translation by the Ministry of Interior is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&keel=en&pg=1&ptyyp=RT&tyyp=X&query=h%E4daolukorra.

factors – and encompasses also events where such consequences are brought about by cyber activities. The definition does not *per se* differentiate whether the emergency is caused by hostile actors (threats) or results from structural conditions or accidents without relation to intent or capabilities of actors (risks).

For the purpose of response, the act foresees a system of measures which includes *preventing* emergencies, *preparing* for emergencies, *responding* to emergencies and *mitigating* the consequences of emergencies ('crisis management').

The responsibilities of emergency response are divided between relevant stakeholders – while the national crisis management committee[112] is responsible for national scale coordination and ensuring emergency preparedness, a system of regional and local committees[113] was set up for operational crisis management in emergency situations of regional or local scale, with the task to ensure the continuity of certain vital services and act as coordinating bodies.

The protection of critical infrastructure – including critical information infrastructure – is addressed in Chapter 4 of the Emergency Act. The chapter identifies 41 services essential to public security, public safety, and the economic and social welfare of people. It also specifies the requirements for ensuring the continuous operation of these vital services and the division of tasks between stakeholders for this purpose.

Management and coordination functions for ensuring sectoral service continuity are divided between different ministries in accordance with their spheres of competence, with the Ministry of the Interior functioning as the central coordinating body. Their purpose is to ensure the following:

a) avoiding wide-scale disruption of the continuous operation of vital services *(prevention)*;

b) the availability of sufficient measures to swiftly eliminate disruptions or launch alternatives *(reaction)*;

c) adequate preparedness of both public and private sector to restore the continuous operation of vital services *(consequence management)*.[114]

The task of individual ministries is to coordinate emergency preparedness activities, advise and supervise the actual entities providing vital services, and keep the Ministry of Interior regularly updated about the situation in their area of

112 The crisis management Committee of the Government of the Republic. The Committee is a permanent body under the Government, chaired by the Minister of the Interior; its members are appointed by the Estonian government. The tasks of the Committee are defined in § 3 of the Emergency Act.

113 § § 4 and 5 of the Emergency Act, respectively.

114 Ministry of the Interior, Department of crisis management and rescue policy. Elutähtsad valdkonnad ja teenused. http://www.siseministeerium.ee/elutahtsad-valdkonnad-ja-teenused-2/ (In Estonian).

responsibility.

The "top layer", i.e. ministry-level management tasks related to ensuring services that are vital for the functioning of information society is divided among different ministries according to their daily competence share; there is no body specifically appointed with the managing the continuity of information infrastructure-related services across service sectors. Overseeing the continuous functioning of communications networks – including fixed and mobile telephone networks, data communications networks, and cable television networks – lies within the sphere of competence of the Ministry of Economic Affairs and Communications.

However, the act also places a burden of day-to-day emergency prevention and ensuring service continuity on providers of public services such as energy suppliers, hospitals, and, relevant to cyber security, electronic communications service providers and information infrastructure owners.

Providers of vital services, i.e. agencies or legal persons that fulfil a public administration duty defined as a vital service in Chapter 4 or undertakings that provide a vital service listed in Chapter 4 have four main legal obligations regarding emergency preparedness:

1) obligation of preparing and presenting a continuous operation risk assessment[115];
2) obligation of preparing and presenting a continuous operation plan[116];
3) obligation of notification regarding events significantly disturbing service continuity or an impending risk of the occurrence of such events;
4) obligation to provide information to supervisory bodies upon the latter's request.

The continuous operation risk assessments and continuous operation plans are to be presented, for the first time, by 1 January 2011. Uniform guidelines for preparing both of these documents were established by the Minister of the Interior in June 2010.

A separate provision stipulates the obligation of each provider of a vital service to ensure the continuous application of security measures with regard to the

115 See § 38 of the Emergency Act. A *continuous operation risk assessment* is a document describing the *risks* causing a partial or complete interruption in the provision of vital services, the *probability* for such an event, and the *possible consequences* of a partial or complete interruption in the provision of the vital service. The risk assessment is to be regularly assessed for up-to-dateness and amended as necessary.

116 See § 39 of the Emergency Act. A *continuous operation plan* is a document describing the *measures* that need to be taken to prevent and mitigate partial or complete interruptions in the provision of vital services and restore the continuous operation of vital services in the event of a disruption.

information systems used for the provision of vital services, and related *information assets*. The requirements for such specific security measures for vital service information systems and related information assets are to be established by the Government of the Republic by January 2011.

Legislative Review: a Summary

A legal framework that fully supports the objectives of a secure information society needs to comprehensively cover several aspects of law belonging to different legal disciplines. These can be illustrated by the following graph:

CONSTITUTIONAL LAW

FUNDAMENTAL RIGHTS AND FREEDOMS;
ORGANISATION OF THE STATE;
EXECUTION OF PUBLIC AUTHORITY

PRIVATE LAW	PUBLIC ADMINISTRATIVE LAW	CRIMINAL LAW	CRISIS MANAGEMENT LAW	WAR-TIME LAW / NATIONAL DEFENCE LAW
Information society services	General administrative procedure law supporting the accessibility of information society	Substantive criminal law	Critical infrastructure protection (CIP)	National defence organisation
eComms infrastructure provision	Availability of public information and public e services	Criminal procedure law	Critical information infrastructure protection (CIIP)	National defence in peacetime
Provision of eComms services to end users	Data processing and data protection	International cooperation		National defence in conflict/ wartime
General private law supporting the functioning of information society (eCommerce, digital signatures)				

As appears from the division above, the post-2007 legal amendments involved most

of the fields of law depicted, most substantially criminal law (including aspects of criminal procedure) and crisis management law. While not directly involving the second column of the graph above, these amendments are closely tied to it, aiming to strengthen the accessibility of information society as well as the availability of public information and public e-services.

In parallel to the review of crisis management law, the Ministry of Justice was tasked[117] to revise the State of Emergency Act[118] which addresses the preparation for and response to emergencies arising from military threat. This task was chiefly undertaken to ensure the up-to-dateness of the State of Emergency Act in the changed legal and factual environment since the adoption of the act in 1996 – concerning which the street riots and cyber attacks of spring 2007 served as a major wake-up call – but also to ensure consistency between the laws dealing with non-military (Emergency Act) and military threats (State of Emergency Act).

Some updates were also required in legal acts usually classified as private law – in this case, the Electronic Communications Act. The amendment concerned the keeping of log files for online user activities (the so-called data retention obligation foreseen by the European Union data retention directive[119]). Namely, the relevant provisions in the Electronic Communications Act which were intended to ensure that data is retained with regard to the source, destination, date, time and duration of a communication concerning, among other, Internet access, Internet e-mail and Internet telephony, foresaw no liability for cases where communications undertakings failed to meet this obligation. Neither was this liability included in other acts, such as the Penal Code. In practice, this often meant that log files that were required by the police for pre-trial criminal proceedings were either missing or the data contained therein was unreadable.[120] With the amendment, the relevant liability was added in § 184[1].

117 Explanatory Memorandum to the draft act, section 2: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/rtf&file_id=574992&file_name=ErSS%20ja%20KMS%20muutmine%20seletuskiri%20(449).rtf&file_sise=36279&mnsensk=448+SE&fd=2010-04-22 (in Estonian).

118 Erakorralise seisukorra seadus (RT I 1996, 8, 165; 2009, 39, 260). Unofficial English text of the act is available at: http://www.legaltext.ee/text/en/XX10024.htm (update pending).

119 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, 13.4.2006, pp. 54-63.

120 Explanatory Memorandum to the Act amending the Electronic Communications Act (424 SE) (In Estonian), available at: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=535868&file_name=elektroonilise%20side%20muutmine%20seletuskiri%20(424).doc&file_sise=31650&mnsensk=424+SE&fd=2010-04-22.

POLICY

The policy response to the cyber attacks has been diverse: Estonia has initiated several national projects with great significance[121], fostered international cooperation with a number of international organisations[122], as well as paid more attention to the regulation of information society as a whole.[123]

Partly in response to the attacks, and partly due to already undertaken initiatives, the government was determined to outline the Estonian Information Society Strategy 2013[124] and the Implementation Plan 2007-2008 of the Estonian Information Society Strategy[125], as well as draft the Estonian Cyber Security Strategy[126] with a set of additional implementation documents. Additionally, since 2007, elements of the cyber security domain and the need for a more effective regulation have been increasingly mentioned in the strategies of other domains, such as the Guidelines for Development of Criminal Policy until 2018[127] and its explanatory documentation[128] that define long-term objectives and activities on the basis of which the public sector shall plan and perform its activities.

Adopting the Cyber Security Strategy

The adoption of the Cyber Security Strategy has been probably one of the most important undertakings in terms of national security since 2007. The committee in charge of the drafting and adoption of the document consisted of a number of public institutions such as the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Economic Affairs and Communications,

121 List of IT-related projects in Estonia, RISO, available at: http://www.riso.ee/en/information-policy/projects.
122 E.g. Estonia Supports Council of Europe in Fight Against Cyber Crime, Estonian Ministry of Foreign Affairs press release, available at: http://www.vm.ee/?q=en/node/9315; Foreign Minister Paet Invited EU and Southeast Asian Nations to Co-operate in Backing Cyber Defence, Estonian Ministry of Foreign Affairs press release, available at: http://www.vm.ee/?q=en/node/9512; National Experts Shared Cyber Security Recommendations with UN Secretary General, Estonian Ministry of Foreign Affairs press release, available at: http://www.vm.ee/?q=en/node/9722.
123 E.g., Cyber Security Strategy, Information Society Strategy 2007-2013. See more, 5.3.1, 5.3.2.
124 Estonian Information Society Strategy 2013, available at: http://www.epractice.eu/files/media/media_186.pdf.
125 Implementation Plan 2007-2008 of the Estonian Information Society Strategy. Available at http://www.riso.ee/en/information-policy/policy-document/implementation_plan.
126 'Cyber Security Strategy'. Cyber Security Strategy Committee, Ministry of Defence. Tallinn 2008. The English version of the Estonian Cyber Security Strategy is available at: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf.
127 Guidelines for Development of Criminal Policy until 2018, available at: http://www.just.ee/orb.aw/class=file/action=preview/id=50603/Kriminaalpoliitika+arengusuunad+aastani+2018.pdf.
128 Explanatory documentation to Guidelines for Development of Criminal Policy until 2018, available at: http://www.just.ee/orb.aw/class=file/action=preview/id=50604/Seletuskiri+(kriminaalpoliitika+arengusuunad+aastani+2018).pdf.

the Ministry of Internal Affairs and the Ministry of Education and Research. [129] The implementation and overall efficiency of the strategy will be assessed by the Cyber Security Council of the Security Committee of the Government of the Republic.[130] The strategy was presented to the Government and adopted in May 2008.

The practical implementation of the strategy is described in more detail in the implementation plans, which focus on the concrete actions and funds needed to achieve the goals of the Strategy in four main areas: protection of critical information infrastructure and establishment of relevant national systems; increasing competence in cyber security; formation of legal framework for ensuring cyber security; bolstering international co-operation, and raising awareness on cyber security. An Implementation Plan of the strategy for the period of 2008–2010 was compiled, taking into account the suggestions from different state agencies, interest groups and committees, and adopted in May 2009.[131]

In a nutshell, the strategy underlines that the asymmetric security risk of cyber attacks results in inherent vulnerabilities of cyberspace and reflects a global issue that can effectively be solvable only by coordinated actions of all nations. The strategy suggests implementing organisational, technical and regulatory information security measures, as well as aims to developing an over-arching and sophisticated *cyber security culture*.[132]

The strategy aims to fulfil five strategic policy objectives[133]:

a) The development and large-scale implementation of a system of security measures;

b) Increasing competence in cyber security;

c) Improvement of the legal framework for supporting cyber security;

d) Bolstering international cooperation; and

e) Raising awareness on cyber security.

Information Society Strategy 2007-2013

In July 2009, the Government of Estonia approved the amended version of the

129 'Cyber Security Strategy'. Cyber Security Strategy Committee, Ministry of Defence. Tallinn 2008. The English version of the Estonian Cyber Security Strategy is available at: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf.
130 *Id.*
131 'Valitsus kiitis heaks küberjulgeoleku strateegia rakendusplaani aastateks 2009–2011'. Postimees, 14 May 2009 *(In Estonian).* Available at: http://uudisvoog.postimees.ee/?DATE=20090514&ID=204872.
132 'Cyber Security Strategy', p. 3.
133 *Id.*, p. 27-34.

"Estonian Information Society Strategy 2007-2013"[134], an updated policy paper, the first version of which had already been adopted by the government in 2006. The update mainly concerned the measure identified in its section 4.1.1, "Broadening technological access to digital information", to which a chapter was added on the development of broadband Internet access (the EstWIN project[135]).

In 2010, the Implementation Plan for 2010-2011 of the Estonian Information Society Strategy 2007-2013 followed. The document sets out six priority areas: increasing the knowledge, skills and participation of individuals; development of Estonia's next generation broadband network; development of electronic business environment; development of public services; large-scale uptake of e-ID; increasing the interoperability of state information systems. Implementation plan for the years for 2011–2013 is currently under development.

National Security Concept of Estonia

The National Security Concept of Estonia[136] was approved by the Parliament in May 2010, replacing the previous version from 2004. The framework document introduces the objective, principles and directions of the security policy, and emphasises among other global security developments the growing dependence of countries' resilience on the use of cyberspace.[137] As cyberspace may well be used to incite tension and conflicts within a nation, the importance of sufficiently protecting the information technology and communications systems is underlined. The concept separately mentions the need for preventing and combating cyber crime by the means of enhanced cooperation between agencies, developments on legislation and endorsement of public awareness.[138]

134 *Supra note* 64.
135 The objective of the Estonian Broadband Development Foundation (founded in 2009 by the initiative of Ministry of Economic Affairs and Communications and by the members of Estonian Association of Information Technology and Telecommunications) is to launch the project EstWin and give all residential houses, businesses and authorities the possibility to connect to the next-generation broadband network with a transmission speed up to 100 Mbit/s by the year of 2015. "In the scope of EstWin project more than 6000km of fiber-optical cables will be installed and more than 1400 connection points will be constructed. The construction of basic network should provide that 98% of the residential houses, businesses and authorities are located closer than 1.5 km from the basic network". Read more, Estonian Broadband Development Foundation, available at: http://www.elasa.ee/.
136 National Security Concept of Estonia (2010), available at: http://www.kmin.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf.
137 *Id.* p. 6.
138 *Id.* p. 17.

REVIEWING THE ORGANISATIONAL FRAMEWORK

Estonian Informatics Centre

Organisation of the Estonian Informatics Centre

The Estonian Informatics Centre is a state agency administered by the Ministry of Economic Affairs and Communications (MEAC) in general coordination of state information policy and public sector IT development as defined in the national strategy for information society development[139].[140]

The core tasks of the Centre are the coordination of execution of development plans for Estonian information society, development and administration of the components supporting state information systems and ensuring their security, and coordinating incident handling Estonian in computer networks. Since September 2009, the Centre is also responsible for managing and coordinating activities related to the information security of state information systems and Estonian critical information infrastructure. The Centre is the core body responsible for the functioning of information society services provided by the state and the development and administration of intra-governmental data communications services and infrastructure. Additionally, the Centre is the national implementing body for European Union structural aid programs.

The Centre consists of six departments, one of which is the Estonian Computer Emergency Response Team (CERT-EE), and another deals with critical information infrastructure protection.

CERT-EE and Its Role

The Computer Emergency Response Team of Estonia (CERT-EE) has, since its setup in 2006, been the entity responsible for the management of security incidents in .ee computer networks and the national contact point for international co-operation in the field of IT security. CERT operationally handles security incidents that take place in Estonian computer networks, takes measures to prevent such incidents, and works to raise the security awareness of end-users. On state level, CERT's tasks are performed by the Department for Handling Information Security Incidents of the Estonian Informatics Centre.[141]

139 Estonian Information Society Strategy 2013, *supra note* 64.
140 See also the introduction provided at the website of the Estonian Informatics Centre: http://www.ria.ee/about.
141 CERT Estonia, available at: http://www.cert.ee/.

In the 2007 cyber attacks, the CERT naturally became the coordinating body for response to the attacks, engaging system administrators and experts both within and outside of the country. While the legal categorisation of the incident and the suitable legal remedies were still discussed, technical measures such as increasing the bandwidth of affected targets and filtering out malicious traffic were applied as measures available under the Electronic Communications Act in cases of harmful interference and negative effects to the integrity of communications networks.[142] These activities were carried out by network and service providers in close cooperation with the CERT.

Even though the technical coordination in incident handling worked well *ad hoc*, questions nevertheless remained unanswered. The authority to coordinate response to or recovery from major cyber attacks was divided between different government entities. The CERT is subordinated to the MEAC. The coordination of matters related to terrorism has so far been the concern of the Ministry of Internal Affairs, while national security matters are handled mainly by the Ministry of Defence. In order to avoid conflicting responsibilities and ensure a streamlined response, the coordination needs to be based on a clear legal regime. As the foundation for a coherent response framework was established with the new Emergency Act in 2009 (see the discussion under section 5.2.3 of this paper), the implementation of the Act will continue to place a stronger burden on the CERT and the Estonian Informatics Centre in general, especially on its department of critical information infrastructure protection.

Department of Critical Information Infrastructure Protection

Due to the adoption of the Emergency Act and the necessity for a competent body to advise and coordinate the matters of protection of critical information infrastructure, the Estonian Informatics Centre was expanded by a new entity – the department of Critical Information Infrastructure Protection (CIIP Department). While the advisory function had *de facto* been fulfilled by the Centre already prior to the setup of the new unit, the Centre now had dedicated staff[143] and a clear-cut tasking to manage and coordinate the creation and operation of a defence system for Estonia's critical information infrastructure.

The CIIP Department is to deal with the protection of important IT systems of the

142 § § 98 and 127 of the Electronic Communications Act. Unofficial English translation available at: http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=et&sk=en&dok=X90001K2.htm&query=elektroonilise%20side&tyyp=X&ptyyp=RT&pg=1&fr=no.

143 As of the start of the department in October 2009, the staff included two people (head of department and a risk manager), with plans to increase the number of staff in future.

public and private sectors alike, coordinating general prevention and response activities while the owners of each vital service concerned remain responsible for the daily defence of their systems. According to Toomas Viira, head of the department, the setup of the new department was called by a need for a central unit to analyse the threats and risks against various information services vital to the state, as well as the influence of various IT systems on one another. The CIIP Department will be able to give recommendations on improving the defence of information systems.[144]

Compared to the more operational role of CERT-EE, the CIIP Department will function at a more strategic level, and thus complement the existing capabilities of the Estonian Informatics Centre to include a fuller competence.

Restructuring the Estonian Informatics Centre

In May 2010, the Government supported the proposal of the Ministry of Defence to reform the Estonian Informatics Centre, upgrading it from a ministry-administered state agency into a government agency with autonomous executive powers.[145] The new regulatory body is to be better empowered to enforce the principles defined by the national cyber security strategy, thus ensuring a greater degree of coherence and better efficiency in its implementation.

According to the Minister of Defence quoted in the article cited above, the tasks of the new authority would comprise monitoring and regulating undertakings that own and run critical information infrastructure, as well as supervising other governmental agencies dealing with information infrastructure. Granting additional mandate to the Estonian Informatics Centre would serve as a long-term investment for cyber security in Estonia, both in terms of ensuring a higher level of information security on the national scale and facilitating international cooperation in the field.

The name of the new governmental organisation and the number of new staff to be recruited is not yet fully determined, but there is an initial agreement that the reform would be completed and the new body launched by January 2011.

Cyber Defence League

The cyber events in April-May 2007 awakened a discussion in Estonia about the potential role for voluntary efforts of defending information infrastructure in the

144 EIC creates unit for defence of critical information systems. Press release by the Estonian Informatics Centre, 30 Sept 2009. http://www.ria.ee/eic-creates-unit-for-defence-of-critical-information-systems.
145 Pesur, Veiko, Infosüsteemide arenduskeskus saab võimu juurde, Postimees Online, 13 May 2010, available at: http://www.postimees.ee/?id=262349.

event of cyber attacks. The concept received support in the 2008 Cyber Security Strategy, and first units of the Cyber Defence League (also *CDL*) were activated in early 2009.[146]

The Cyber Defence League operates as a part of the Defence League, a voluntary military national defence organisation founded already in 1918 (and restored in 1990) whose traditional purpose has been to enhance the readiness of the nation to defend its independence and its constitutional order, including in the event of military threat, but also by supporting civil structures such as the rescue service and police.[147] The Cyber Defence League functions within the same framework, with a mission to protect the high-tech lifestyle of the country, defending information infrastructure and working to raise awareness, share best practices, improve cooperation (incl. across the private and public sector) and create a network of specialists that are able to support mitigation efforts in the case of a cyber incident.[148]

In addition to its routine daily task of improving awareness and competence, the Cyber Defence League can be used in emergency response, rescue work and in ensuring security. The conditions and procedure for their involvement are specified in the Emergency Act: the CDL may be used for performing emergency situation tasks, as well as preventing or restraining acts of terrorism (including via cyber means) and preventing or restraining the damaging of high-risk objects. The precondition for the CDL's involvement is the inability of a competent agency to perform the duty in a timely manner and the absence of other means to perform the duty; in any case, the CDL has to follow the procedure established by the Government of the Republic.[149]

The Cyber Defence League unites IT specialists in key positions, patriotically minded people with IT skills that are willing to make a contribution to the cyber defence of the nation, and experts of various other disciplines that support cyber defence.[150]

As of spring 2010, the Cyber Defence League included about 60 members.[151]

146 Jaagant, Urmas. Küberkaitseliit pakub harjutuskeskkonda vabatahtlikele IT-spetsialistidele. EPL Online, 14 April 2010. http://www.epl.ee/artikkel/575013.
147 See the introduction about the Defence League at http://www.kaitseliit.ee/index.php?op=body&cat_id=288.
148 *Küberkaitseliit*. National Defence League's website, http://www.kaitseliit.ee/index.php?op=body&cat_id=395; KKK. National Defence League's website, http://www.kaitseliit.ee/index.php?op=body&cat_id=396.
149 See § 31 of the Emergency Act (an unofficial English translation is available at http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=et&sk=en&dok=XXXXX26.htm&query=h%E4daolukorra&tyyp=X&ptyyp=RT&pg=1&fr=no).
150 See supra note 115.
151 Randlaid, Sven, Küberkaitseliit soovib oma liikmeskonda laiendada, ERR, 15 April 2010. http://uudised.err.ee/index.php?06200567.

CONCLUSION

High level of IT development and the inevitable dependency on information technologies determine the need to protect nations against cyber attacks, be they criminal or military by nature. Although the attacks in Estonia in 2007 were not *per se* regarded as cyber war, they made the Estonian authorities review the existing cyber security concept and come up with a comprehensive strategy for protecting the information society.

The attacks triggered modifications in the Estonian legislative situation, organisational structure as well as institutional landscape. Following the legal analyses undergone for the new cyber security strategy and the implementation plan, there were several changes made in the Penal Code. The modifications itemised in more detail the provisions relating to attacks against computer systems and data, updated the scope of some provisions (such as adding the dissemination of spyware and malware) and added a new provision on preparation of cyber crimes. The amendments also prescribed higher maximum punishments and corporate liability for such crimes.

The new Emergency Act was adopted to offer legal remedies and contingency planning for critical information infrastructure. The aim of the act is to comprehensively address all national emergency situations, laying a foundation for a uniform organisational emergency handling structure and procedural framework for emergency response. National cyber security threats were thus included under the general framework set up by the act. Certain provisions also specifically address threats against information systems.

From organisational perspective, the central governmental body responsible for government information systems as well as the Estonian national CERT, was supplemented by the Department for Critical Information Infrastructure Protection (CIIP). The tasks of the new department include creating a defence system for Estonia's critical information infrastructure and the protection of important IT systems of the public and private sectors alike. The Emergency Act will continue to place a stronger burden on the CERT and the Estonian Informatics Centre in managing cyber security.

The Cyber Defence League was created with a mission to protect the high-tech lifestyle of the country, defending information infrastructure and working to raise awareness, share best practices, improve cooperation (e.g. between the private and public sector) and create a network of specialists that are able to support mitigation efforts in the case of a cyber incident. It functions as a part of the Defence League, a voluntary military national defence organisation founded already in 1918 (and

restored in 1990) whose traditional purpose has been to enhance the readiness of the nation to defend its independence and its constitutional order, including in the event of military threat, but also by supporting civil structures such as the rescue service and police.

The analysis of the policy, legal and organisational aftermath of the Estonia 2007 cyber attacks concludes that in order to achieve a comprehensive set of effective measures for preparedness, response and mitigation in the field of cyber security and defence, the arguments deriving from all three fields of law – LOAC, Criminal Law and IT Law – must be combined in an over-arching response. Additionally, by engaging several areas of government in cyber security capability building and integrating policies and views on cyber security, Estonia has taken its cyber security planning and preparedness a level higher from the previous, information-society focused approach.