

Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security

Christian Czosseck, Rain Ottis and Anna-Maria Talihärm
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Christian.Czosseck@ccdcoe.org

Rain.Ottis@ccdcoe.org

Anna-Maria.Talihärm@ccdcoe.org

Abstract: At the time of the state-wide cyber attacks in 2007, Estonia was one of the most developed nations in Europe regarding the ubiquitous use of information and communication technology (ICT) in all aspects of the society. Relying on the Internet for conducting a wide range of business transactions was and still is common practice. Some of the relevant indicators include: 99% of all banking done via electronic means, over a hundred public e-services available and the first online parliamentary elections in the world. But naturally, the more a society depends on ICT, the more it becomes vulnerable to cyber attacks. Unlike other research on the Estonian incident, this case study shall not focus on the analysis of the events themselves. Instead it looks at Estonia's cyber security policy and subsequent changes made in response to the cyber attacks hitting Estonia in 2007. As such, the paper provides a comprehensive overview of the strategic, legal and organisational changes based on lessons learned by Estonia after the 2007 cyber attacks. The analysis provided herein is based on a review of national security governing strategies, changes in the Estonia's legal framework and organisations with direct impact on cyber security. The paper discusses six important lessons learned and manifested in actual changes: each followed by a set of cyber security policy recommendations appealing to national security analysts as well as nation states developing their own cyber security strategy.

Keywords: Estonia, cyber attacks, lessons learned, strategy, legal framework, organisational changes

1. Introduction

Over three weeks in the spring of 2007, Estonia was hit by a series of politically motivated cyber attacks. Web defacements carrying political messages targeted websites of political parties, and governmental and commercial organisations suffered from different forms of denial of service or distributed denial of service (DDoS) attacks. Among the targets were Estonian governmental agencies and services, schools, banks, Internet Service Providers (ISPs), as well as media channels and private web sites (Evron, 2008; Tikk, Kaska, & Vihul, 2010).

Estonian government's decision to move a Soviet memorial of the World War II from its previous location in central Tallinn to a military cemetery triggered street riots in Estonia, violence against the Estonian Ambassador in Moscow, indirect economic sanctions by Russia, as well as a campaign of politically motivated cyber attacks against Estonia (Ottis, 2008). By April 28th the cyber attacks against Estonia were officially recognized as being more than just random criminal acts (Kash, 2008). The details of the weeks that followed are described in (Tikk, Kaska, & Vihul, 2010).

The methods used in this incident were not really new. However, considering Estonia's small size and high reliance on information systems, the attacks posed a significant threat. Estonia *did not* consider the event as an armed attack and thus refrained from requesting NATO's support under Art. 5 of the NATO Treaty; instead, the attacks were simply regarded as individual cyber crimes (Nazario, 2007; Tikk, Kaska, & Vihul, 2010) or "hacktivism" as established by a well-known information security analyst Dorothy Denning (Denning, 2001). A further discussion on whether or not the 2007 attacks were an armed attack is beyond the scope of this paper. Many defence and security analysts have covered this particular topic and discussed e.g. the "juridical notion of information warfare" (Hyacinthe, 2009), a "taxonomies of lethal information technologies" (Hyacinthe & Fleurantin, 2007), formulated a "Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict" (Brown, 2006), or "legal limitations of information warfare" (Ellis, 2006).

The incident quickly drew worldwide attention, and media labelled the attacks the first "Cyber War" (Landler & Markoff, 2007). This led to an overall "cyber war hype" that was continuously carried forward by media, researchers and policymakers. This exaggerating rhetoric was employed during following conflicts like Georgia 2008 or Kyrgyzstan 2009, and such misuse of terminology has already received a fair amount of criticism (Farivar, 2009).

The 2007 attacks have shown that cyber attacks are not limited to single institutions, but can evolve to a level threatening national security. Looking back, the Estonian state was not seriously affected since to a larger extent state functions and objects of critical information infrastructure were not interrupted or disturbed (Odrats, 2007). However, nation states did receive a wake-up call on the new threats emerging from cyber space, alongside with new types of opponents.

The following three sections will provide a comprehensive overview of major changes in Estonia's national cyber security landscape, namely the changes of national policy. As a result, several laws and regulations were introduced, while others were amended, and there were several changes in the organisational landscape.

This paper features six lessons learned that were identified as most remarkable in the case study of Estonia. It concludes with several strategic cyber security recommendations.

2. Development of national strategies

The benefits as well as threats of the use of Internet-related applications to information societies are identified by a number of Estonian high level policies and strategies.

The *Estonian Information Society Strategy 2013* (MoEAC, 2006), in force since January 2007, promotes the broad use of ICT for the development of a knowledge-based society and economy. Given that cyber attacks on a scale matching that of Estonia in 2007 were unseen and likely unpredicted so far, it is not surprising that the risk of massive cyber attacks was not taken into serious consideration in the strategy – nor in other national policy documents from that era (see e.g. the implementation plan of the Information Society Strategy for 2007-2008, MoEAC, 2007)

The *National Security Concept* of Estonia published in 2004 (MoD, 2004) and the government's action plan in force at this time (Estonian Government, 2007) were no exception since these documents did not even mention possible cyber threats or related actions.

It was only after the 2007 cyber attacks that cyber security instantly found its way into the national security spotlight.

2.1 Policy and strategy responses since 2007

In July 2007, shortly following the cyber attacks, the Government approved the *Action Plan to Fight Cyber-attacks* (Kaska, Talihärm, & Tikk, 2010). In September 2007, the revised Implementation Plan 2007-2008 of the Estonian Information Society Strategy 2013 (MoEAC, 2007) was approved. The document holds a generic statement that critical information infrastructure should be developed in such a way that it operates smoothly in “emergency situations” (Mol 2009).

2.1.1 Cyber security strategy

In May 2008, the Estonian government adopted the newly drafted *Cyber Security Strategy* (CSS) as a comprehensive policy response to the cyber attacks. The strategy was prepared by a multi-stakeholder committee including relevant ministries, agencies and private sector representatives.

The CSS considers cyber security a national effort responding to the asymmetric threat posed by cyber attacks. The strategy underlines that state-wide cyber security requires active international cooperation and the promotion of global responses. On a national level, the strategy suggests implementing organisational, technical and legal changes. Further, it aims at developing an over-arching and sophisticated *cyber security culture* (MoD, 2008).

Based on a post-attack assessment of the situation in Estonia, the CSS identified five strategic objectives:

- The development and large-scale implementation of a system of security measures;
- Increasing competence in cyber security;
- Improvement of the legal framework for supporting cyber security;
- Bolstering international cooperation; and
- Raising awareness on cyber security.

In May 2009, the CSS implementation plan for the 2009-2011 cycle was adopted by the government. The plan called for concrete actions in five priority areas and became the main source for the comprehensive cyber security approach in Estonia (Estonian Government, 2009).

2.1.2 National Security Concept

The *National Security Concept*, which was updated and approved in May 2010, represents Estonian government's second major cyber security policy response. It recognizes Estonia's growing reliance on ICT along with the increasing threat posed by terrorists and organised crime groups. Cyber crime should receive special attention, and solutions are to be found in co-operation between agencies on both national and international level. Cyber security shall be ensured by "[...] reducing vulnerabilities of critical information systems and data communication connections". Critical systems shall stay operational, even if the connection to foreign countries is temporarily malfunctioning or has ceased to function. To support these actions, the necessary legislation should be developed and public awareness raised (MoD, 2010). The National Security Concept led to the revised *Guidelines for Development of Criminal Policy until 2018*, published in October 2010. The Police shall focus on preventing the spread of malware and the growing number of "hacking" incidents. Furthermore "[t]he existence of a sufficient number of IT specialists in law enforcement agencies shall be ensured in order to set bounds to cyber crime more efficiently." (MoJ, 2010). Other strategies like the *Estonian Information Society Strategy 2007-2013* have received only minor cyber security related amendments.

In addition, since the 2007 attacks, Estonia has become one of the major advocates of cyber security on the international level. As one result, NATO initiated the development of a unified strategy against cyber attacks (Blomfield, 2007) and in 2010 NATO adopted the new strategic concept that recognizes cyber attacks as a threat to the alliance and opts for the enhancement of alliance's and nations' capabilities to face the threat (NATO, 2010).

Moreover, Estonia has actively supported a number of international organisations such as the Council of Europe in its fight against cyber crime (MoFA, 2010a), Association of Southeast Asian Nations in promoting the harmonization of laws concerning cyber crime (MoFA, 2010b) and United Nations in contributing an expert to the task force on *Developments in Information and Communication Technology in the Context of International Security* (MoFA, 2010c).

3. Development in the legal field

The 2007 attacks prompted major changes in the Estonian legislative landscape and in some cases enhanced the changes already underway. Legal amendments involved several areas of law related to cyber security (see Table 1): criminal law (including aspects of criminal procedure) and crisis management law. The Estonian incident did not, however, directly touch upon the legal regime applicable to armed conflicts since the attacks were treated by national authorities as acts of crime.

Other laws such as the Electronic Communications Act were also updated but did not involve considerable changes in the context of cyber security (Estonian Government, 2010). *Table 1.*(Kaska, Talihärm, & Tikk, 2010)

Table 1: Law related to cyber security

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)				

3.1 Penal code

Mostly due to the need to harmonize the Estonian Penal Code with the *Council of Europe Convention on Cyber Crime* (Council of Europe, 2001) and the Council Framework Decision 2005/222/JHA of on attacks against information systems (Council of Europe, 2005) all cyber crime related provisions in the Penal Code were reviewed. The amendments targeted the provisions addressing attacks against computer systems and data, widened the scope of specific computer crime provisions (e.g. criminalizing the dissemination of spyware and malware), added a new offence of the preparation of cyber crimes, modified the provision concerning acts of terrorism and filled an important gap (Estonian Government, n d) 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 of the state) and ordinary computer crime (Mol, 2009).

3.2 Amendments relevant to criminal procedure law

The amendments in the Penal Code resulted partly from the regulatory limitations that arose in relation to the application of the Code of Criminal Procedure (CCP) to the 2007 attacks (MoJ, 2010b) as CCP §§ 110-112 maintain that evidence may be collected by surveillance activities in a criminal proceeding if the collection of evidence 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 (MoJ, 2010b). However, during the Estonian attacks in 2007 it became apparent that almost none of the committed offences met the threshold of "three years" imprisonment and that precluded the employment of surveillance measures (Estonian Government, 2007b). Therefore, the changes in the Penal Code prescribed higher maximum punishments and also corporate liability for cyber crime offences.

3.3 New Emergency Act

The new Emergency Act (EA) (Mol, 2009) was adopted in June 2009 and reviewed the current setup of national emergency preparedness and emergency management structure, including the responses to cyber threats.

Offering a comprehensive approach, the act foresees a system of measures which include preventing emergencies, preparing for emergencies, responding to emergencies and mitigating the consequences of emergencies ("crisis management") (Mol, n d). It is the providers of public services and information infrastructure owners that are tasked with everyday emergency prevention and ensuring the stable level of service continuity. Providers of vital services are obliged, among other assignments, to prepare and present a continuous operation risk assessment (EA § 38) and an operation plan (EA § 39) to notify the citizens about events significantly disturbing service continuity as well as to provide the necessary information to supervisory bodies. In addition to the above, there are certain provisions that specifically address threats against information systems, such as an obligation for the providers of vital services to guarantee the smooth application of security measures in information systems and information assets used for the provision of vital services.

4. Development of organisations

Before the 2007 cyber attacks Estonia had relatively few organisations dedicated to (national) cyber defence. Since then, Estonia has made some key organisational changes to better deal with the cyber threats. The most significant ones are described below.

A high level organisational change was the formation of the *Cyber Security Council* under the Government Security Committee, a body foreseen by the National Cyber Security Strategy. The Council reports directly to the Government Security Committee and is therefore well-placed for coordinating inter-agency and international cyber incident response.

4.1 EIC, CERT-EE and CIIP

Estonian Informatics Centre (EIC) is a state agency that is responsible for managing and developing public information services and systems (MoEAC, 2009). It is also tasked with providing cyber security for these services and systems. Even though a national CERT had been established in 2006 as a department of the EIC, its capabilities and experience were still quite modest at the time of the attacks. In 2009, as a result of the National Cyber Security Strategy, the Department of Critical Information

Infrastructure Protection (CIIP) was added to the structure of EIC, in addition to the already existing CERT. The main tasks of the new department include supervising risk analyses of critical information infrastructures and developing protective measures.

4.2 Cyber defence league

During the cyber attack campaign, the Estonian CERT was assisted by an informal network of volunteer cyber security experts. This provided much needed additional capabilities, such as increased situational awareness, analysis capability, quick sharing of defensive techniques between targeted entities, as well as an extended network of direct contacts to international partners.

The roots of this informal group derive from the late 1990ies, when Estonia was adopting a national ID card system. Over the years, the network of professionals had also cooperated against criminally motivated cyber attacks targeting critical infrastructures (e.g., Estonian banks). A later development was the formalisation of this loose cooperation into the Cyber Defence League (CDL) in 2009. The Defence League is a volunteer national defence organization in the military chain of command. The CDL is part of the Defence League and unites cyber security specialists who are willing to contribute their time and skills for the protection of the high-tech way of life in Estonia, especially assisting the defence of critical information infrastructure. It is important to note that this is a defensive organisation, not designed to harass political adversaries in (anonymous) cyber attack campaigns. In January 2011, the CDL was reorganized into the Cyber Defence Unit of the Defence League, but the CDL name is still widely used.

CDL's key activities include organizing training and awareness events, as well as cyber defence exercises. In 2010, the CDL was involved with the Baltic Cyber Shield exercise organised by Cooperative Cyber Defence Centre of Excellence (Geers, 2010), the US-led International Cyber Defence Workshop, as well as a series of national exercises. The CDL is a good example of managing in a productive manner the expertise and enthusiasm of motivated cyber security specialists.

5. Six recommendations

Given that the major changes have been discussed above, the next section will feature six significant lessons learned from the 2007 cyber attacks against Estonia:

5.1 Comprehensive strategy approach

It is evident that Estonia has taken into account the lessons learned from the 2007 incident, the most significant step being the quick establishment of a comprehensive policy response which has led to the adoption and subsequent implementation of the national Cyber Security Strategy. The Estonian example emphasises the need for nation-wide cooperation and countermeasures against cyber crime, involving major stakeholders of the public and private sector.

It remains to be debated whether cyber security should be handled in a single comprehensive strategy or form a sub-section of all other relevant strategies touching upon ICT. However, considering the speed of technological advancements and comparing it with the speed of developing national strategies, the Estonian approach of having a single strategy might be the one more advisable.

The 2007 attacks triggered the cyber security strategy drafting in Estonia. However, countries should not wait for such triggers and should pro-actively conduct a thorough and comprehensive risk assessment of their cyber infrastructure. Furthermore, often only the context and additional information will reveal if the attack was launched with crime, espionage, terrorism or military motivation. Therefore, close cooperation between relevant agencies remains a *sine qua non* to success in this arena.

5.2 Politically motivated cyber attacks

Another aspect to consider is the shift of attention in terms of cyber security threats over the last decade. While the first half of the decade the cyber security focus was on criminal and espionage attacks (if recognised as a national security issue at all), the second half witnessed a surge in politically motivated cyber attacks (Nazario, 2009). The significance of this development is that targets have transformed. A politically motivated attacker is likely to attack visible and politically significant targets (such as the public website of a government agency or a company that has angered an interest group), which are of little interest to criminals and intelligence agencies. This shift in targets requires everyone to reassess their risks and security requirements.

Politically motivated actors can cover the entire spectrum of cyber attack, from high-profile strikes against critical infrastructure, to millions of pinprick attacks that can weaken the state over a long period of time (Lemay, Fernandez, & Knight, 2010; Liles, 2010; Ottis, 2009). As the threat of politically motivated attacks threatening national security is not likely to go away in the foreseeable future, it must be addressed as a national security issue in order to get the full attention of policymakers.

5.3 Legal recommendations

An analysis of the Estonian legal order governing the domain of information society underlines that a secure information society needs to be comprehensively supported by norms involving several legal disciplines. The broad approach illustrated by the Estonian legal framework brings together the areas of private and public law, and completes the spectrum of cyber incident regulation by engaging criminal law, crisis management regulation and wartime law/national defence legal order. It is vital for countries to realize that the international cyber security regulation involves a wide range of legal areas and the review of relevant regulatory frameworks and the identification of possible uncovered “grey areas” is highly recommended.

Within national legal systems, a review of criminal law (penal law) appears to be a central issue. Attacks against critical (information) infrastructure, politically motivated cyber attacks, possible cases of cyber terrorism, as well as related provisions for investigation and prosecution, should all be reflected in the domestic criminal law or other national acts. Broad and inclusive national implementation of the *Council of Europe Convention on Cybercrime* is of crucial importance, especially considering the cross-border nature of cyber crime.

Additionally, the Estonian experience underlined the need to establish common security standards for all computer users, information systems and critical infrastructure companies (MoD, 2008). By 2011, steps have been taken to establish such standards for service providers within the framework of the Electronic Communications Act, but more detailed rules for end-users’ conduct and/or legal obligations are still needed.

5.4 Exercises and education for the masses

A key component of enhancing (national) cyber security is cyber security awareness and education. This should not be limited to professionals in governmental or private institutions, but must cover the whole spectrum from a citizen using ICT for everyday things to senior policy makers, considering the skills and knowledge needed at every level. This includes law enforcement agencies and especially the judicial system that has a central role in interpreting the regulatory aspects of cyber security. By developing different solutions well suited for each groups, a *broad and sophisticated cyber security culture* can be implemented, as aimed for in the CSS.

Estonia recognized its lack of sufficient number of well-trained information security experts and developed a new Master’s program for Cyber Security Studies in 2008. The *Cyber Defence League* is another venue for actively training experts in cyber security. Further measures, such as information campaigns for the secure use of the Internet, special classes in high school or vocational training should be considered by Estonia and other nation states.

Additionally, cyber security exercises organised both on national and international level serve as effective preparation to respond to cyber attacks. Exercises like *Cyber Europe 2010* (ENISA, 2010) require efficient coordination between agencies and private shareholders and should be regularly conducted.

5.5 International relations

The attacks against Estonia in 2007 underlined the importance of international cooperation as it became even more apparent that in the context of responding to cyber threats, one country can do little alone. To that end, active participation in the work of major organizations dealing with cyber security requires keeping national developments and legal framework up to date and serves as a useful ground for new initiatives, further collaboration and regional or global forum. Moreover, the ratification of instruments such as the Council of Europe Convention of Cyber Crime that aim to harmonise cyber crime regulation worldwide should be supported and promoted.

Beside the political will for cooperation, national multi- and bilateral agreements, information sharing agreements, cooperation of law enforcement agencies, joint investigation teams, international exercises, formal and informal networks and other international initiatives are vital for effective prosecution and investigation of cyber crime offences.

5.6 Harnessing the volunteers

It is well known that most of the Internet infrastructure is owned and operated by the private sector. It follows that there is a pool of experts in the private sector, who could provide a meaningful contribution to national cyber security, regardless of their actual position in the private sector. This also includes experts in the public sector, who do not work in their area of expertise. Clearly, there are limits to the use of volunteers, whether their potential role is in offensive or defensive activities (Ottis, 2009). However, if proper legal, policy and operational frameworks are in place, volunteers can significantly increase national cyber security capability.

6. Conclusions

While in hindsight, the cyber attacks against Estonia were not as severe as often referred to, they still triggered an understanding of threats from cyber space as threats potentially affecting national security and prompted a wake-up call concerning the risks associated with the “careless use” of digital information technologies (e.g., Internet). For instance, the risk posed by politically motivated individuals should be regarded as a possible element of a serious threat to cyber security. By reviewing the strategic, legal and organisational changes that Estonia has undergone after the 2007 cyber attacks, this paper provides a concise list of key changes that have taken place on the legislative and administrative levels. While this paper describes some new assets that so far appear to be unique to Estonia, such as the formation of the Cyber Defence League, it offers several recommendations to national security planners performing beyond Estonia’s national boundaries. Many of the aforementioned recommendations are not new; but they have passed a practical test through the real-life Estonian case study. Accordingly, these recommendations are more than a set of purely theoretical proposals. Lastly, based on the foregoing analysis, it is important to stress the fact that cyber security of a nation state can only be achieved by an interlocked approach covering national policies, its legal framework and organisations involving both public and private actors, as well as necessary changes identified by a realistic risk assessment.

Disclaimer

The opinions expressed here are those of the authors and should not be considered as the official policy of the Cooperative Cyber Defence Centre of Excellence or NATO.

Acknowledgement

We would like Mrs. Kadri Kaska and the unknown reviewer for their substantial comments they provided us with in the course of writing this paper.

References

- Blomfield, A. (2007). Estonia calls for Nato cyber-terrorism strategy. Retrieved from <http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html>.
- Brown, D. (2006) “A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict”, *Harvard International Law Journal*, 47 (1), 179-221.
- CDL. (n.d.). Cyber Defence League. Retrieved from http://www.kaitseliit.ee/index.php?op=body&cat_id=395.
- Council of Europe. (2001). Convention on Cybercrime. Retrieved from <http://conventions.coe.int/treaty/en/treaties/html/185.htm>.
- Council of Europe. (2005). Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. *Official Journal L* 69, 67-71.
- Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, 239–288.
- Ellis, B. (2001) “The International Legal Implications and Limitations of Information Warfare: What Are Our Options?”. Retrieved Mar. 2, 2011 from http://www.iwar.org.uk/law/resources/iwlaw/Ellis_B_W_01.pdf.
- ENISA. (2010). EU Cyber Security Exercise ‘Cyber Europe 2010’. Retrieved January 31, 2011, from <http://www.enisa.europa.eu/media/press-releases/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded>.
- Estonian Government. (2007a). Programme of the Coalition for 2007-2011.
- Estonian Government. (2007b). Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code (116 SE) (In Estonian). Retrieved from http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20090902161440&

- file_id=198499&file_name=KarS_seletuskiri (167).doc&file_size=66048&mnsensk=166+SE&etapp=03.12.2007&fd=29.10.2008.
- Estonian Government. (2009). Valitsus kiitis heaks küberjulgeoleku strateegia rakendusplaani aastateks 2009–2011. Retrieved from <http://uudisvoog.postimees.ee/?DATE=20090514&ID=204872>.
- Estonian Government. (2010). Explanatory Memorandum to the Act amending the Electronic Communications Act (424 SE) (In Estonian). Retrieved from http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=535868&file_name=elektroonilise_side_muutmise_seletuskiri_424.doc&file_size=31650&mnsensk=424+SE&fd=.
- Evron, G. (2008). Battling botnets and online mobs: Estonia's defense efforts during the internet war. *Georgetown Journal of International Affairs*, 9(1), 121–126.
- Farivar, C. (2009). A Brief Examination of Media Coverage of Cyberattacks (2007 - Present). In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber warfare* (pp. 182 - 188). IOS Press.
- Geers, K. (2010). Live Fire Exercise: Preparing for Cyber War. *Journal of Homeland Security and Emergency Management*, 7(1).
- Hyacinthe, B. (2009). *Cyber Warriors at War*. Xlibris, pp. 82-85.
- Hyacinthe, B. & Fleurantin, L. (2007). Initial supports to regulate information warfare's potentially lethal information technologies and techniques. *Proceedings of the 3rd International Conference on Information Warfare and Security* (pp. 206-207). Academic Conferences Limited.
- Kash, W. (2008). Lessons from the cyberattacks on Estonia. Retrieved from <http://gcn.com/articles/2008/06/13/lauri-almann--lessons-from-the-cyberattacks-on-estonia.aspx>.
- Kaska, K., Talihärm, A.-M., & Tikk, E. (2010). Building a Comprehensive Approach to Cyber Security. CCD COE Publications.
- Landler, M., & Markoff, J. (2007). In Estonia, what may be the first war in cyberspace. *The New York Times*. Retrieved from <http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html>.
- Lemay, A., Fernandez, J. M., & Knight, S. (2010). Pinprick attacks, a lesser included case? In C. Czosseck & K. Podins (Eds.), *Conference on Cyber Conflict Proceedings* (pp. 183 - 194). Tallinn: CCD COE Publications.
- Liles, S. (2010). Cyber Warfare: As a form of low-intensity conflict and insurgency. In C. Czosseck & K. Podins (Eds.), *Conference on Cyber Conflict Proceedings* (pp. 47 - 57). Tallinn: CCD COE Publications.
- MoD. (2004). National Security Concept of the Republic of Estonia.
- MoD. (2008). Cyber Security Strategy. Retrieved from http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.
- MoD. (2010). NATIONAL SECURITY CONCEPT. Retrieved from http://www.kmin.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf.
- MoEAC. (2006). Estonian Information Society Strategy 2013. Retrieved from http://www.riso.ee/en/system/files/Estonian_Information_Society_Strategy_2013.pdf.
- MoEAC. (2007). Implementation Plan 2007-2008 of the Estonian Information Society Strategy.
- MoEAC. (2009). Statute for the Development of National Information System (in Estonian). Retrieved from <https://www.riigiteataja.ee/akt/13219897>.
- MoFA. (2010a). Estonia Supports Council of Europe in Fight Against Cyber Crime. Retrieved from <http://www.vm.ee/?q=en/node/9315>.
- MoFA. (2010b). Foreign Minister Paet Invited EU and Southeast Asian Nations to Co-operate in Backing Cyber Defence. Retrieved from <http://www.vm.ee/?q=en/node/9512>.
- MoFA. (2010c). National Experts Shared Cyber Security Recommendations with UN Secretary General. Retrieved from <http://www.vm.ee/?q=en/node/9722>.
- Mol. (2009). Estonian Emergency Act (unofficial translation). Retrieved January 4, 2011, from <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&keel=en&pg=1&ptyyp=RT&tyyp=X&query=h□daolukorra>.
- Mol. (n.d.). Ministry of the Interior, Department of crisis management and rescue policy (in Estonian). Retrieved January 4, 2011, from <http://www.siseministeerium.ee/elutahtsad-valdkonnad-ja-teenused-2>.
- MoJ. (2010a). Guidelines for Development of Criminal Policy until 2018. Retrieved from <http://www.just.ee/arengusuunad2018>.
- MoJ. (2010b). Estonian Code of Criminal Procedure (unofficial translation). Retrieved from <http://www.legaltext.ee/text/en/X60027K6.htm>.
- NATO. (2010). Strategic Concept for the Defence and Security of the Members of the NATO. Retrieved December 30, 2010, from http://www.nato.int/cps/en/natolive/official_texts_68580.htm.
- Nazario, J. (2007). Estonian DDoS Attacks – A summary to date. Retrieved from <http://asert.arboretworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>.
- Nazario, J. (2009). Politically Motivated Denial of Service Attacks. In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 163-181). 163-181: IOS Press.
- Odrats, I. (Ed.). (2007). *Information Technology in the Public Administration of Estonia Yearbook 2007*. Ministry of Economic Affairs and Communication.
- Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare* (p. 163). Academic Conferences Limited.
- Ottis, R. (2009). Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. *8th European Conference on Information Warfare and Security* (pp. 177-182). Academic Publishing Limited.
- Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations* (p. 130). Tallinn: CCD COE Publications.