DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
35

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
35

ENEKEN TIKK

Comprehensive legal approach to cyber security

TARTU UNIVERSITY PRESS

Faculty of Law, University of Tartu, Estonia

Dissertation is accepted for the commencement of the degree of *doctor iuris* on June, 29 2011, by the Council of the Faculty of Law.

Supervisor: Prof. Raul Narits (University of Tartu)

Opponents: Prof. Dr. Marco Gercke (Institut für Medienstrafrecht)

Commencement will take place August 3, 2011 at 12.00 in the Faculty of Law, Näituse 20 room K-03

Publication of this dissertation is supported by the Faculty of Law, University of Tartu

ISSN 1406–6394
ISBN 978–9949–19–762–0 (trükis)
ISBN 978–9949–19–763–7 (PDF)

Tartu Ülikooli Kirjastus
www.tyk.ee
Tellimus nr 465

To
General Ants Laaneots

CONTENTS

LIST OF ABBREVIATIONS

AF	Air Force
ARPANET	Advanced Research Projects Agency Network
CCD COE	Cooperative Cyber Defense Centre of Excellence
CI	Critical Infrastructure
CII	Critical Infrastructure Information
CNA	Computer Network Attack
CNCI	Comprehensive National Cybersecurity Initiative
CND	Computer Network Defense
CNO	Computer Network Operation
CNE	Computer Network Exploitation
COE	Council of Europe
DNS	Domain Name System
DOD	Department of Defense
EDI	Electronic Data Interchange
EU	European Union
ICJ	International Court of Justice
ICT	Information and Communication Technology
IHL	International Humanitarian Law
INSS	Institute of National Security Studies
ISP	Internet Service Provider
IT	Information Technology
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organisation
NDU	National Defense University
NCIRC	NATO Computer Incident Response Capability
NIS	Network and Information Security
OCS	Office of Cyber Security
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Cooperation in Europe
RRT	Rapid Reaction Team
SLA	Service Level Agreement
UN	United Nations
US	United States
WSIS	World Summit on the Information Society

INTRODUCTION

The need for a comprehensive approach to cyber security deriving from the architecture of the Internet and emerging cyber security threats and incidents requires a systematic development, interpretation and application of legal areas and instruments. Legal instruments in the field of information society and telecommunications, cyber crime, national security and armed conflict, if developed and applied in a consistent and systematic manner, will diminish currently existing gaps in regulation and reduce inconsistencies in legal interpretation.

The author compares and correlates comprehensive approach-related findings by legal, policy and technology experts and proposes a structural and substantive framework for addressing the full spectrum of cyber security. This thesis develops a framework for assessing the quality of existing law from a comprehensive cyber security perspective. This work is intended to lead to gradual decrease of the divide between purely academic and practical approaches, a more homogenous understanding and implementation of law by legal, policy and technology communities and a defined scope for additional regulation.

Over the past few years cyber security has turned into a strategic issue[1] forcing nations to revise their goals and capabilities and requiring the attention of information technology experts, national policy makers, diplomats, military commanders and intelligence communities managing these emerging security challenges. For each of these stakeholders, cyber security is not a completely new domain, but a growing concern introducing significant new challenges and complex issues. As Nissenbaum explains it: „Over the course of the past decade, the mandate of computer security has grown in complexity and seriousness as information technologies have saturated society and, simultaneously, the threats have multiplied in number and sophistication".[2] Nissenbaum notes: „[C]yber-security overlaps with technical security but encompasses more".[3] Borg goes further, concluding that the information society has reached a revolutionary phase where its defence requires the revision of all principles, strategy, tactics and decision-making processes.[4]

Chapter I of this dissertation will elaborate on the development of the cyber threat and security paradigm and will provide a factual and analytical background for the conclusions and proposals of Chapters II and III.

---

[1] See, e.g. Kenneth Geers. Strategic Cyber Security. – CCD COE Publishing 2011. Alexander Klimburg, Heli Tiirmaa-Klaar. Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU. – European Parliament, 2011.

[2] Helen Nissenbaum. Where computer security meets national security. – Ethics and Information Technology, 2005, No. 7, pp. 61–73.

[3] *Ibid*.

[4] Scott Borg. The Cyber-Defense Revolution – A Synthesis (2009). Available at http://www.ccdcoe.org/cyberwarfare/images/234.pdf (last accessed June 25, 2011).

With politically motivated cyber incidents on the rise, and critical national information services and infrastructure threatened by increasingly sophisticated malicious activity, cyber security has grown into an immediate area of concern for national governments and international organizations. Analysis of the deterrence mechanisms and security measures developed so far has indicated that because of the architecture of the Internet and the setup of information society, no country or international organization is in the position to come up with all-encompassing solutions and responses for cyber security.

As a result of the convergence of threats, targets and responses, and the acknowledgment of their fragmented mandate, capabilities and resources, nations and international organizations have recognized the need for an approach that combines the experience, expertise, capabilities and resources of all areas and levels of cyber incident handling. Such an effort is called a comprehensive approach. Although not a technical term in itself, the concept has been widely adopted and advocated as a common denominator for mutually reinforcing initiatives that enhance the security of cyberspace.

Acknowledged on the international level only in the past few years, national calls for a broad approach to cyber security date back almost a decade. One of the first countries to call for a comprehensive cyber security initiative on the governmental level was the United States. Later, the same approach was adopted by Estonia, the United Kingdom and several other countries. On the international level, policy statements in support to a coordinated effort have recently been made by the EU, OSCE and NATO.

Although adopted as a strategic and policy goal by major international organizations and many nation states, a comprehensive approach cannot be merely regarded as a policy catch-phrase. The comprehensive approach to cyber security has also been recognized by technology experts as a tool for addressing the complexity of cyber threats and defences. Even before the 2007 Estonian attacks that led to international focus on these issues, Nissenbaum observed that computer security has turned into a national security issue and that the differences between these two conceptual approaches are significant for regulation and the design of technology.[5]

An approach combining considerations of threat, deterrence and response from different areas of authority and responsibility, thereby aiming at eliminating gaps between different aspects of cyber incident prevention, detection, response and recovery, has been identified by several legal scholars as a workable way to overcome gaps in regulation and legal practice.

The need for a coordinated legal approach exists for several reasons. First, unlike earlier conflict environments, the information infrastructure on which governments, military and the information society rely, is mostly privately owned. This means that the military capabilities required to respond to a "cyber armed attack" will necessarily involve infrastructure owned and operated by the private sector. Therefore defences against and responses to cyber attacks will

[5] *Supra nota* 2, 63.

depend to a great extent on systems and security standards designed in peace time with primarily commercial interests in mind. This is so because national security threats have emerged now when the critical mass of global networking platforms has already been invested into, and the underlying architecture is very difficult, if not impossible, to restructure. From a legal perspective, this means that national legal approaches to data and consumer protection and due diligence by information system operators and communication service providers, will determine law enforcement and national defence capabilities in case of a cyber incident of relevant scope and nature. Therefore, for example, data protection requirements and data retention techniques and standards, although developed under different areas of law and coordinated by different national authorities, essentially need to be regarded as aspects of the availability and quality of data about cyber incidents.

Secondly, without a comprehensive approach, the authority to respond to and handle an incident remains unclear. As Westby explains, at the time of a cyber attack, it is not possible to immediately determine whether the attacker is a script kiddie, an insider, a rogue actor (organized crime, terrorist organization, or radical), or a nation state. Therefore, the "response baton" may have to be passed from the private sector to law enforcement to the military with swift, efficient coordination and certainty regarding legal authority for actions taken.[6] Without the implementation of a comprehensive response approach, the legal authority of communication service providers, national Computer Emergency Response Teams, law enforcement and military will remain disconnected and benefit malicious actors.

Thirdly, without coordinated legal remedies and enforcement mechanisms it is easy for the malicious actors to identify and exploit the gaps in legal responses and remedies. Without a systematic and correlated analysis of the requirements for information system security standards and the liability of operators and users, criminalized offenses and trends in cyber criminal law, national security exceptions to information society-related rights and freedoms such as the privacy and freedom of information and speech as well as options for holding nation states and their proxies accountable, the existing legal frameworks do not deter but rather create opportunities for malicious actors.

Also, with little interaction between law, technology and policy, the responses to incidents remain inefficient. Without deeper consideration of information and communications technology, legal interpretation lacks clarity and certainty. Blume observes: "[law] must be balanced and respect the fact that there are social reasons for applying technological developments."[7] Without under-

[6] Jody Westby. Homeland Security v Homeland Defense: Gaps Galore. – Paper for St. Mary's Universiry School of Law, Center for Terrorism Law Seminar „State Open Government Law and Practice in a Post-9/11 World: Legal and Policy Analysis. November 2007. Available at http://www.globalcyberrisk.com/pdfs/St%20Marys%20-%20Homeland%20Defense%20Gap%20Paper%20v5.pdf (last accessed June 10, 2011).

[7] Peter Blume. Information Infrastructure and Data Protection. The Danish perspective. – International Journal of Law and Information Technology, Vol. 4 No. 1, 1996, pp. 1–18.

standing these reasons and the technology itself, it will be difficult to establish and enforce an acceptable balance. Blume's conclusions complement Reidenberg's opinion that a body of "*lex informatica*" has evolved based on the set of rules on information flows imposed by technology and communication networks.

For these reasons this dissertation does not question the need for a comprehensive approach to cyber security. Instead, the author elaborates on the background, scope and elements of such an approach and how the corodinated efforts of different disciplines can be supported legally. In doing this, the author focuses primarily on a de lege lata approach, using recently developed legislative and interpretative practices to promote international discussions on the applicability of the existing legal framework. The author hypothesizes that, in order to support a comprehensive approach to cyber security, concepts of law relevant to the spectrum of cyber threats and defences need to be developed and applied in a consistent and systematic manner so as to diminish the gaps in regulation and reduce inconsistencies in legal interpretation.

The observations by legal scholars about the need for a more systematic and coordinated way of responding to global cyber threats need to be addressed in conjunction with the architecture of the Internet, the current cyber threat situation and lessons learned from past incidents. Considering the architecture of information society infrastructure and services, as well as the evolving range of malicious activities and targets, it has been accepted that a compartmentalized approach to cyber security fails to satisfy the requirements for the functioning of the information society and that a coordinated approach involving different disciplines, levels of authority, and methods needs to be taken.

This thesis compares and correlates comprehensive approach-related findings by legal, technology and policy experts with the aim of proposing a structural and substantive framework for addressing the full spectrum of cyber security in a non-fragmented and non-compartmentalised way from the legal perspective. Without prejudice to the potential need for additional regulation of cyber security on the international level, this thesis develops a framework for assessing the quality of existing law and thereby gradually narrowing the scope of international treaty negotiations.

The author asserts that without cross-disciplinary legal analysis and practice there is insufficient clarity as to the need for additional regulation, since the interpretative limits of the existing legal framework have not been examined. With reference to Eckstedt, the author takes the view that the analysis conducted using the conceptual framework offered in this thesis will indicate the need for additional regulation.

While extensive academic literature exists in the field, workable mechanisms are needed to adapt to the current cyber threat picture. The need for a more practical (or just a different) approach has been advocated by many legal scholars in the past few years (e.g. Ophardt, Barkham, Waxman, Broadhurst and others). Curiously, the same conclusions have been reached in virtually all

areas of law relating to the spectrum of cyber security.[8] To promote these discussions, the author brings together in Chapter III the legal issues and concepts that she considers most important for supporting the comprehensive approach to cyber security.

A challenge for writing this dissertation is that there is no commonly agreed definition of a comprehensive approach. There are, however, a few defined approaches to contemporary cyber threats. OSCE has concluded that a comprehensive approach is based on the understanding that the widespread use of the Internet by terrorists, traffickers and criminals makes it increasingly difficult to develop effective responses to transnational threats without promoting a more secure cyberspace. A comprehensive approach to cyber security should: (a) strengthen national security; (b) tackle cybercrime; (c) inhibit terrorist use of the Internet; (d) respond to a wide variety of risks and threats, including politico-military; and (e) enable competent authorities to protect a wide spectrum of targets ranging from the individual Internet user to critical infrastructures; and (f) safeguard the Internet as a space for free expression and assembly. In the Estonian National Cyber Security Strategy a comprehensive approach is seen as the protection of a country's entire cyber assets involving all sectors of national society, a clear and efficient allocation of responsibilities therein for the prevention of cyber attacks, and increased general competence and awareness regarding threats in cyberspace.

The author has overcome the lack of a uniform understanding by explaining in Chapter I the elements of a comprehensive approach as referred to in the existing definitions and then offering her own interpretative model of the comprehensive approach in Chapter II.

She has hypothesised that implementing the goals and principles identified as part of a comprehensive approach from the legal perspective requires identifying legal areas, concepts, authority and instruments addressing all elements of a such approach and then combining and balancing the existing legal practices and interpretations so as to reflect the gaps and possible controversies affecting the implementation of a comprehensive approach to cyber security. The author has therefore concluded that from the legal perspective there is a structural and instrumental aspect to a comprehensive approach and has explored these in detail in Chapters II and III.

Without the dimension of national security in cyber security thinking, the legal and policy framework has developed to respond primarily to the needs of the electronic communications market and the necessary conditions for individual rights and freedoms. Legal concepts like privacy and freedom of speech support anonymity and non-attribution – the widely recognised rights in information society that in the context of national security would need to be subjected to significant restrictions. This is not to say that there are no legal

[8] See, e.g. Vida M. Antolin-Jenkins. Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places? – Naval Law Review. Vol. 51, 2005, pp. 132–174.

remedies to threats to national security and warfare – those bodies of law have not yet been restated from the cyber security perspective and therefore the implementation of national security law and the law of armed conflict in the domain of cyber security is an emerging legal topic.

Considering the changed threat situation and the divide between national experiences and cyber capabilities and priorities, elaborating a new international normative base for cyber security would be beyond any subject matter area expert's capability.

Within relatively homogeneous cyber security risk environments in the past, emphasis has been put on organisation- and area-specific approaches to competences and available legal remedies, thus interpreting norms within each specific legal field rather than in an interdisciplinary context. With the occurrence of systematic politically motivated cyber attacks and considerable national efforts towards cyber warfare capabilities, the notion of cyber security has developed and the legal accommodation of cyber security risks needs also to be interdisciplinary and coordinated.

The latter combined with the recent guidance from international organisations and national cyber security strategic decisions gives a reason to elaborate a comprehensive legal approach to cyber security, i.e., an approach to cyber security aspects and issues combining the concepts and remedies of areas of law relevant to different stages and types of cyber incidents.

Against the background of the changed cyber security situation in terms of targets, motivation and levels of authority involved in mitigating the incidents, a comprehensive legal approach needs to involve these factors in future legal argumentation and solutions and at the same time acknowledge the already existing legal framework related to information society, electronic communications, cyber crime, threats to national security and armed conflict. In consequence, combining existing legal concepts and their interpretations with the changed cyber conflict paradigm, and bridging legal argumentation and remedies of different areas of legal expertise as well as integrating the underlying theory and practice of other areas of expertise involved in cyber incident handling enables the constructive discussion of the deficiencies in current legal interpretation and argumentation and define the qualitative and quantitative need for a legislative change in relation to cyber security.

More importantly, the structure and comprehensibility of legal order and argumentation are the key factors of legal certainty. The latter, in turn, is the immanent condition of the effective functioning of the society in general.

The central argument of this thesis is that a comprehensive legal approach to cyber security requires a systematic and coordinated regulatory and interpretative methodology across the legal disciplines governing telecommunications, cyber crime, national security and international peace and security as well as between different levels of authority.

Hence, this dissertation argues that the existing models of addressing cyber security, focusing primarily on the market and cyber crime, are incomplete and fragmentary, whether they are intended to address cyber crime or intrusions

with political motivation and context. A fragmented approach is not adequate for the current and emerging cyber threat picture and, as indicated by recent incidents, fails to deter cyber malicious activity especially in the domain of national security, but also cyber crime.

The author also hypothesises that the claimed inadequacy of the existing legal framework to respond to current cyber security threats has developed due to the shift of the cyber conflict paradigm. The author further argues that the contemporary notion of cyber security produces novel implementation and interpretation of existing cyber security legal instruments. The author observes that legal remedies to current cyber security posture derive from and are manifested in different legal areas, each being relevant at a certain stage of a particular incident. The author observes that the immaturity of practical legal thinking in some areas of cyber conflict complicates the international discussion on cyber security related agreements. The author does not, *per se*, rule out the need for an international agreement on cyber security. The dissertation underlines the legal aspects supporting and framing such treaty and elaborates on legal policy challenges potentially affecting international discussions.

Against these hypotheses, the author first analyzes how the notion and scope of cyber security have changed within the past decade. Chapter I will show that cyber attacks targeted against critical information infrastructure do not correspond to the logical threat assessment of each individual target and are not directly associated with the business model of each individual target, thus rendering the individual cyber security plans ineffective in case of a multi-target attack. It further concludes that due to the relatively recent acknowledgement of the need for a comprehensive approach, this approach requires the adjustment of different perspectives and therefore the revision of a number of premises for legal and policy advice in this area. The argument in Chapter I is supported by the case study of the cyber attacks against Estonia in 2007 and cross-referenced to analysis of the attacks against Georgian and Lithuanian information infrastructure in 2008 as well as to legal observations from more recent incidents like WikiLeaks, Stuxnet and Conficker. Showing that in the past few years cyber incidents have developed political and ideological characteristics and considering the fact that nation states have started to develop offensive cyber capabilities, Chapter I concludes that cyber security has developed from a merely computer science concern into an arena comprising elements of social life, business, criminality, national security and, potentially, warfare. This conclusion, along with a comparative analysis of major international organisations' cyber security agendas, leads to the designing of a structural framework for international cyber security in Chapter II.

Chapter II, recognizing that neither a single nation's or organisation's unique experience or any area of cyber incident handling (especially law) alone can serve as a model for restructuring global cyber security regulatory thinking, introduces a framework of elements and perspectives to be considered when revising the regulatory approach towards the new cyber security paradigm. En large, it elaborates on the structural components of a comprehensive approach

from legal and policy perspective abstracted in the conclusions of Chapter I. Chapter II therefore designs a structural framework for developing legal solutions for the current cyber security posture. It envisages the components of a comprehensive regulatory approach to cyber security by shaping the current cyber security paradigm, legal areas and key legal concepts involved as well as the authorities and responsibilities involved in designing cyber security. The need for interaction between law, information technology and policy has been emphasised as the key to viable and practical legal approaches to cyber conflict. Further emphasis is put on the requirement for interdisciplinary legal analysis whereby information society and electronic communications law, criminal law and proceedings, national security law and the law of armed conflict form a symbiosis of different bodies of law for cyber security purposes.

Chapter III takes the observations from Chapter I into an instrumental and substantive legal context and intends to create concrete discussion points for the legal, policy and technical communities on the quality of existing legal practice in order to support a comprehensive cyber security approach. Chapter III reflects the author's view of how different legal concepts, principles and practices based on the current research in the field, the experience of nations which are victims of politically motivated cyber attacks, and the recent expert discussions at international conferences and workshops, form a spectrum of legal instruments and concepts applicable to the full spectrum of cyber security. The ambition of Chapter III is to add focus on discussions between experts and thereby take the analysis and argumentation further from mere acknowledgment of issues and obstacles. That is why instead of listing legal issues, aspects or concepts, the author has worded a set of rules that will invoke debate and discussions on the limits and practices under existing legal frameworks. Chapter III provides an analytical legal framework for resolving common cyber security related issues. Based on the analysis of existing international legal instruments and principles supporting or affecting cyber security capabilities, it suggests that the gaps in relevant legal frameworks are qualitative rather than quantitative. It finally offers a concept of Cyber Security Rules of Behaviour aiming at an interdisciplinary legal-technological-policy discussion on the quality of law and the concepts available to governments for improving the level of national cyber security.

To create further discussion around the proposed framework the author has taken a provocative view and instead of merely pointing out legal issues, has adopted the approach recommended by Prof. Heintschel von Heinegg and written a set of legal statements based on the existing legal instruments and their recent interpretation. In doing so, the author calls for critical review of these areas of law by legal experts of respective fields in order to achieve a more focused and balanced discussion that, because of the scope and sophistication of the research involved, could not be adequately accomplished by one legal scholar. The author proposes that a discussion encompassing different areas of law would indicate the existing gaps in regulation and point out ways for overcoming them beyond international treaty negotiations. Having analysed a

few of the areas in-depth the author concludes that several legal issues that are practical for cyber security can be overcome by critical interpretation and legislative steps on the national level.

Having conducted extensive studies and consultations on the subject matter, the author concludes that a cross-disciplinary qualitative analysis is required that would bridge relevant legal approaches and allow conclusions on which cyber security concerns need additional attention by the international community, and which issues can and need to be dealt with on the national level. A fragmented approach that does not exhaust and optimise potentially available legal remedies and balance the implementation of legal instruments from different areas involved will not suffice to improve global and national deterrence against and responses to the current cyber threats.

This dissertation is based primarily on applied and interdisciplinary methodology as opposed to doctrinal legal research. The historical research focused on the development and refinement of the international legal instruments governing the use of the Internet and the information architecture. The historical research took place from early 2007 to late 2008. In 2010, the author extended the historical research by conducting a comparative study on Internet-related legal and policy developments in the United States of America and Europe during 1970–2010 vis-à-vis the development of technology and occurrence of cyber incidents. This research created the groundwork for understanding the current cyber conflict trends and provided the original hypotheses for this dissertation.

After the research aimed at identifying the legal instruments and case law addressing different elements of cyber security the results of which have been annexed to this dissertation, the author has used the "mixed methods research", also called "triangulation," in Chapter I to correlate the statistical and survey data about the information society, recent cyber security instruments and international organizations' policy approaches with the conclusions of legal and technology scholars about the need for a comprehensive approach to cyber security. A a pre-text for this dissertation, the author has conducted an extensive quantitative study of elements of the comprehensive approach as understood and accepted by legal, technology and policy experts and legal instruments, case law and legal practices surrounding the uses of information and communications technology. This study has led to the conclusions in Chapter II on legal categorization of cyber incidents, relevant legal areas and instruments, levels of authority and disciplines involved.

The author then has proceeded to conduct a series of events to discuss and develop these findings. Chapter II involves the concepts discussed at the Cyber Conflict Law and Policy Conference organized by the Cooperative Cyber Defense Centre of Excellence in Tallinn on September 9–11, 2009 with 110 participants from 24 countries, and a series of workshops with more than a hundred cyber security experts during 2009 and 2010.

In combination with comparative analysis of relevant legal academic work the author has then identified legal issues that are identified as areas of concern

by authorities, experts and scholars in the field of cyber security. Chapter III is based on the conclusions and discussions of 70 experts on the Legal and Policy Track of the Cyber Conflict Conference organized by the Cooperative Cyber Defense Centre of Excellence in Tallinn on June 13–18, 2010 and followed up by a series of workshops.

Additionally, the author has attended over 40 international academic and expert events to discuss and further develop the hypotheses and key findings presented in this dissertation.

For the purposes of Chapter II the author has combined fundamental research on the legal concepts and institutional structure that potentially support the comprehensive approach to cyber security as explained in Chapter I, with the analysis of the conclusions of recent academic and expert discussions.

The development of the qualitative expert opinion to a great extent relied upon a series of focus group workshops, which fostered the gathering of intellectual expertise and the feedback of experts in both law and cyber security. From 2008 to 2010, eight workshops in cooperation with the George Mason University Center for Infrastructure Protection, the US National Defense University, the US Naval Postgraduate School and national defense ministries, were conducted in the United States, the Netherlands, Sweden, Latvia and Norway, involving more than 100 cyber security legal, policy and technology experts. The workshops focused on the legal considerations of major international cyber incidents from 2007–2009, the Frameworks for International Security, and most recently, the concept of Rules of Behaviour for Cyber Security.

Chapter III is a synthesis of the academic and expert conclusions from a substantive legal perspective. The author has conducted a survey of legal issues surrounding cyber security from information society, criminal law and international law perspectives and combined the observations of legal scholars and practitioners with those of cyber incident handling entities such as law enforcement agencies, policy-makers and diplomats. Combining the results thereof with the conclusions of the instrumental research, the author proposes a topical framework for systematically and cross-disciplinarily addressing the legal aspects of a comprehensive approach cyber security.

The choice of methods corresponds to the conceptual approach taken by the author to an overall legal framework of cyber security instead of an in-depth study of a specific legal issue. Acknowledging cyber security-related law as a developing discipline, the author has made a conscious decision to contrast observations from legal practice with academic legal research and introduce constraints to cyber security-related legal analysis and practice arising from the technology and policy perspectives.

The main conclusions and key content of this dissertation have been presented at a number of international conferences during 2007–2010. Examples include the NATO Information Assurance Symposium (2007, 2010), the US Information Warfare Conference (2009), the Cooperative Cyber Defense Centre of Excellence (hereafter: CCD COE) Cyber Warfare Conference (2009), the NATO Advanced Research Workshop (2009), the CCD COE Legal and Policy

Conference (2009), the European Conference on Information Warfare (2010), the UN Peacekeeping Conference (2010), and the Military Legal Advisers' Conference (2010).

Two international conferences have been organised by the CCD COE specifically to discuss and develop the concepts and approaches presented in this thesis – in 2009, around 120 experts from 24 countries attended the Law and Policy Conference and in 2010, the Law and Policy track of the Cyber Conflict Conference and the pre-conference workshop involved around 100 experts from 39 countries. The concepts and conclusions of this thesis also served as input for the legal track of the CCD COE 2011 International Conference on Cyber Conflict.

The background studies for this dissertation are published by CCD COE Publishing and consist of four compilations in the publication series entitled „Frameworks for International Security": Cyber Security Legal and Policy Instruments (2009), Cyber Security International Case Law (2010), National Cyber Security Policy and Strategy (2011). To indicate the scope and content of the background studies, the author has annexed the tables of contents of these compilations to this dissertation (Annexes 1–3 respectively).

The basis for the observations elaborated on in Chapter I is the book co-authored with Kadri Kaska and Liis Vihul – "International Cyber Incidents: Legal Considerations" (CCD COE Publishing, 2010).

The key arguments and conclusions of this dissertation have been augmented in and are supported by a series of articles on related topics: Applicability of the Census Case in Estonian Personal Data Protection Law, in: Juridica International, 2006, No. 1, pp. 102–110; Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism, in: NATO Science for Peace and Security Series – E: Human and Societal Dynamics, "Responses to Cyber Terrorism", IOS Press, Volume 34, 2008, pp. 89–103; Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective, in: NATO Science for Peace and Security Series – E: Human and Societal Dynamics, "Modelling Cyber Security: Approaches, Methodology, Strategies", IOS Press, Volume 59, 2009, pp. 189–198; Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons (Proceedings of the 9th European Conference on Information Warfare and Security Hosted by Strategyinternational.org and the Department of Applied Informatics University of Macedonia Thessaloniki, Greece 1–2 July 2010. Edited by Josef Demergis, University of Macedonia Thessaloniki Greece), Global Cyber Security – Thinking About Ways Ahead for NATO, SAIS Review – Volume 30, Number 2, Summer-Fall 2010, pp. 105–119 and Ten Rules for Cyber Security, in: Survival: Global Politics and Strategy, Volume 53, no. 3, June-July 2011, pp. 119–132. Additional writings related to this dissertation are published by IEEE ("From Chaos to Collective Defense") and the proceedings of the 2010 Cyber Conflict Conference ("Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation").

Taking into account the numerous articles, compilations and analyses written and edited by the author, this dissertation is written on a more conceptual level in order to appropriately reflect all the relevant conclusions drawn as a result of the author's research.

Annexed to this dissertation are additional supporting studies on relevant definitions (Annex 1).

This dissertation approaches the legal framework to cyber security from the international legal perspective. The analysis and conclusions of the dissertation can, however, with minor modifications be used to analyse national legal and regulatory responses to cyber security.

This work has been possible by contributions and participation of many leading intellectuals from all over the world. Their contribution is gratefully acknowledged. The author wants to thank Professor Raul Narits who encouraged her to engage in this still developing and in many ways uncertain area of research. The author also thanks her colleagues at the CCD COE, US National Defense University and Swedish National Defense College. The author's sincere and kind thanks also go to Dan and Julie Ryan, Maeve Dion, Tom Wingfield, Jude Klena, Irv Lachow, Ulf Häussler, Mike Schmitt, Greg Rattray for their insights and advice. The author deeply values the opportunity provided by Raul Rikk, Ants Laaneots, Aarne Ermus, Ilmar Tamm and Johannes Kert.

The author is indebted to Liis Vihul and Seamus Flory for proofreading and cite-checking this text. She thanks her parents and Paula Johanna for their patience and encouragement. Rene's support and help in the final phase of this work is invaluable.

CHAPTER I.
THE CHANGING UNDERSTANDING OF CYBER SECURITY

"This is the first time in American history that we in the federal government, alone, cannot protect our infrastructure. We can't hire an army or a police force that's large enough to protect all of America's cell phones or pagers or computer networks – not when 95 per cent of these infrastructures are owned and operated by the private sector."
Secretary Dale at White House Press Briefing, January 7, 2000

At a glance nothing truly historic has happened in the world that could require an immediate change in policy and law supporting international peace and security. The increased involvement of different international organisations in international peace missions and the revision of the notion of security have been on-going since the end of the Cold War.[9] The need for integration of civilian and military efforts to secure international peace and welfare has been asserted on the international level numerous times.[10] Also, the appearance of the notion of cyber security in the agenda of nations in the mid–80s[11] and the international organisations in the mid- and late 90s[12] can be seen as a logical continuation of defining and assuring their mandate. Yet the increasing occurrence of politically motivated cyber incidents indicates a new level of maturity of the information society. Cyber threats that have been an integral part of the information society have matured gradually over decades and now call for a "ones and zeros" revision of international peace and security posture.

As Professor Julie Ryan notes, "[t]he development, adoption, dissemination, and widespread use of information processing technologies have engulfed us all, when we were not looking. Now we discover ourselves in a land where the scenery seems familiar but the rules work differently. Civilian and military

---

[9] See, e.g. Ulf Häuβler. Ensuring and Enforcing Human Security: The Practice of International Peace Missions. War or Crime? National Legal Challenges in Europe to the War in Iraq. – Wolf Legal Publishers, 2009, p. 577.

[10] More on this Stephanie Blair. Towards Integration? Unifying Military and Civilian ESDP Operations. – European Security Review No. 44, May 2009. Available at http://www.isis-europe.org/pdf/2009_artrel_272_esr44-civmil-integration.pdf
(last accessed May 5, 2011).

[11] See, e.g., Myriam Dunn Cavelty. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. – Routledge, 2008, pp. 8–9.

[12] Some activities of international organisations in the field of cyber security date back to early 80-ies, but most cyber security agendas for organisations like the EU, Council of Europe, OSCE, OECD, UN, NATO and G8 were developed during 90-ies and revised gradually during the past decade. See more on this Michael Portnoy, Seymour Goodman. Global Initiatives to Secure Cyberspace: An Emerging Landscape. – Springer, 2009. A compilation of international cyber security legal and policy instruments in Eneken Tikk. Frameworks for International Cyber Security: Legal and Policy Instruments. – CCD COE Publishing, 2010.

efforts in pursuit of the global peace and security are increasingly interconnected, integrated, and coordinated. More and more, militaries are formally recognizing the concept of cyber warfare and are developing specialisations in that area[13]. Clearly something important and special is occurring and focusing around 'cyber'."[14]

From the discussions about the adequacy of the current legal and policy framework to respond to contemporary types of cyber attacks and recent revisions of national strategic responses to cyber incidents that the world has recently witnessed, it becomes evident that the cyber security environment is changing[15] and requires additional attention from the national security perspective[16]. Apparently, the legal framework built in the last decade to tackle cyber crime has not proved efficient in the context of national security-relevant cyber incidents like Estonia (2007), Georgia (2008), Conficker (2009), Stuxnet (2010) and many more.[17] Cyber incidents of the past three years indicate that the reliance on information infrastructure and service has developed to a point where it is becoming possible to undermine the functionality of governments and support political objectives of nations.

While for some time, thinking about national security-relevant cyber incidents, and in particular, cyber warfare, was primarily based on semi-fictitious scenarios[18] developed by combining elements of real incidents with theoretical impact and hypothetical motivations, the world has recently witnessed a number of real-life incidents that can and have been used as bases for further studies and analysis. Incidents such as the Morris Worm[19], Solar Sunrise[20], the Cuckoo's

---

[13] See, e.g., Jeffrey Carr. Inside Cyber Warfare: Mapping the Cyber Underworld. – O'Reilly Media, 2009, pp. 37–39.

[14] Prof. Julie Ryan (George Washington University) to the author in a private professional consultation.

[15] See, e.g., Duncan B. Hollis. Why States Need an International Law for Information Operation. – Lewis & Clark Law Review. Vol. 11, 2007, p. 1023; Also, Karol Dobrzeniecki. How Should We Deal with Human rights in Cyberspace? Some Remarks. – International Review of Law Computers & Technology, Vol. 19, No. 3, November 2005, pp. 253–258.

[16] Stein Schjølberg, Solange Ghernaouti-Hélie. A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace. – Cybercrimedata, 2009.

[17] More on national security relevant cyber incidents in Eneken Tikk, Kadri Kaska, Liis Vihul. International Cyber Incidents: Legal Considerations. – CCD COE Publishing, 2010.

[18] See, e.g., Kelly A. Gable. Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. Available at http://works.bepress.com/kelly_gable/2 (last accessed May 5, 2011). Jonathan A. Ophardt. Cyber Warfare and the Crime of Aggression: the Need for Individual Accountability for Tomorrow's Battlefield. – Duke Law and Technology Review. No. 3, 2010. Counter-arguments are provided by Joshua Green. The Myth of Cyberterrorism. – Washington Monthly. November 2002. Available at http://www.washingtonmonthly.com/features/2001/0211.green.html (last accessed May 5, 2011).

[19] United States v. Morris (928 F.2d 504 (2d Cir. 1991)) – Robert Tappan Morris was convicted of releasing a virus into the Internet thereby causing computers at educational institutions and military sites to crash. /.../ Due to Morris' miscalculation, the program developed by him to reveal the deficiencies of current security measures on computer

Egg[21], the US East Coast blackout[22] etc., have been used as bases of hypothetical examples of national security-relevant cyber threats.[23]

Hypothetical thinking about cyber incidents leads to a situation where cyber threats are addressed in a "borrowed context" and they therefore do not result in a realistic threat perception or practical solutions. Despite the fact that dozens of articles have been written in the past two decades on the need to address cyber threats in national legal and policy documents[24], most nations have just recently started looking into the practical national security aspects of cyberspace.[25]
For many nations that are part of the information society, the threat perceptions have emerged from a "foreign" context where the US represents the most exploited target for different incidents as well as – from a national security and military perspective[26] – the most prominent influential think tank for global

---

networks, duplicated itself well beyond Morris' intent. Morris attempted to kill the worm but it was too late to prevent extensive damage.

[20] Solar Sunrise was a series of computer network attacks directed at the US Department of Defense and committed by teenagers from 1–26 February 1998. See more at: http://www.globalsecurity.org/military/ops/solar-sunrise.htm.

[21] Clifford Stoll. The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage. – Doubleday, 1989. It describes a hunt for a computer cracker who broke into a computer at the Lawrence Berkeley National Laboratory.

[22] In 2003 the Northeast blackout essentially shut down New York City and a wide swatch of the East Coast and Midwest, resulting in more than $10 billion in economic loss. Some officials have suggested that hackers may have been responsible for the 2003 blackout despite initial reports that an Ohio generation plant operated by American Electric and Power (AEP) sent a surge into the system that caused a massive, cascading failure. A worm in the plant's non-power systems was said to be coincidental. For more on recent developments on this case see, e.g., Larry Barrett. US Reviewing Cyber Threat to Power Grid. Available at http://www.internetnews.com/government/article.php/3839241/US-Reviewing-Cyber-Threat-to-Power-Grid.htm (last accessed May 5, 2011). Larry Dignan. China's cyber-militia behind US blackouts? Available at http://www.zdnet.com/blog/btl/chinas-cyber-militia-behind-us-blackouts/8960 (last accessed May 5, 2011).

[23] See, e.g., Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo. Information Warfare and International Law. – National Defense University Press. 1998, p. 8.

[24] See, e.g., John Arquilla and David Ronfeldt. Cyberwar is Coming. – Santa Monica, CA: RAND Corporation, 1993. Available at http://www.rand.org/pubs/reprints/2007/RAND_RP223.pdf (last accessed May 5, 2011). Richard W. Aldrich. Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime. – INSS Occasional Paper 32, Information Operations Series, 2000 "The International Legal Implications of Information Warfare. Airpower Journal. Fall 1996, pp. 99–111. Davis Brown. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. – Harvard Int. Law Journal. Vol. 47, No. 1, 2006.

[25] Recently revised national strategic cyber security strategies are compiled in Eneken Tikk. Frameworks for International Cyber Security: National Cyber Security Strategies. – CCD COE Publishing, 2011.

[26] See, e.g., Michael N. Schmitt. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. – Columbia Journal of Transnational Law. Vol. 37, 1998–99, pp. 885–937; Thomas C. Wingfield, James B. Michael. An Introduction to Legal Aspects of Operations in Cyberspace. – Technical Report NPS-CS-04-005, Naval Postgraduate School, Department of Computer Science, Monterey, California, 28 Apr.

cyber security strategy and law. For the US this has been a natural approach and status considering that the Internet was born in the US military laboratories in 1960s.

EU countries, however, have traditionally devised cyber security strategies focused on extending and strengthening the internal market[27]. Thus, their legal and regulatory focus has been less balanced against national security and military involvement in cyber security.

Recently, a group of nations has developed that have "hands-on" experience with cyber attacks and can therefore share their experience. However, lessons learned by Estonia and Georgia remain distant for nations not sharing similar vulnerabilities and political context.

Until 2007 the (inter)national cyber security perspective had not been prioritised by national legislature and policy-makers and often the academic writings on the subject have been seen as visionary and thus have provoked more speculation than constructive responses. A good example of a controversial and distorted notion of the threat is that of cyber terrorism – as Talihärm[28] observes, the great gap between the presumed danger and the known cyber terrorist activities triggers most of the debates around cyber terrorism: some believe that cyber terrorist attacks are a realistic scenario[29], while others doubt the seriousness of the threat.[30] As Talihärm further explains, Dorothy Denning estimated in 2007 that the threat of cyber terrorism was not higher than in 2001.[31] On the other hand the US Congress was recently warned by a

---

2004; Dorothy E. Denning. Information Warfare and Security. – Addison-Wesley, 1999; Clay Wilson. CRS Report for Congress: Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Available at http://www.fas.org/irp/crs/RL32114.pdf (last accessed May 5, 2011).

[27] E.g., Principles of Estonian Information Policy 2004–2006. Available at http://www.epractice.eu/files/media/media_259.pdf; The Strategy on the Development of the Information Society in Poland for the years 2004–2006. Available at www.mswia.gov.pl/download.php?s=56&id=806 (last accessed May 5, 2011). Strategy of the Republic of Slovenia in the Information Society. Available at http://www.epractice.eu/files/media/media_329.pdf (last accessed May 5, 2011).

[28] Anna-Maria Talihärm. Cyber Terrorism: in Theory or in Practice? – CCD COE Publishing, 2011. Available at http://www.ccdcoe.org/articles/2010/Taliharm_CyberTerrorism.pdf (last accessed May 5, 2011).

[29] Paul Vixie. Cyberterrorism isn't so much a threat to national security as a threat to civilisation. – Newsweek, 2003. Available at http://www.newsweek.com/id/60300 (last accessed May 5, 2011). Eugene E. Habiger. Cyberwarfare and Cyberterrorism: The Need for a New US Strategic Approach. – The Cyber Secure Institute, 2010. Available at http://cybersecureinstitute.org/docs/whitepapers/Habiger_2_1_10.pdf (last accessed May 5, 2011).

[30] Gabriel Weimann. Cyberterrorism: How Real Is The Threat? – Special Research Report, Washington DC: United States Institute of Peace, 2004. Available at http://www.usip.org/pubs/specialreports/sr119.html (last accessed May 5, 2011).

[31] Dorothy Denning. A View of Cyberterrorism Five Years Later. – Readings in Internet Security: Hacking, Counterhacking, and Society (K. Himma ed.), Jones and Bartlett

growing threat of a crippling attack on telecommunications and other computer networks and FBI director Robert Mueller claims that the cyber terrorism threat is „rapidly expanding".[32] The notion has been addressed by several authors[33] and a number of authorities[34] although it is unknown whether any target-oriented[35] cyber attacks of a terrorist nature have occurred anywhere in the world to date.[36] Moreover, as no internationally agreed definition of "terrorism" exists, talking about "cyber terrorism" has no defined focus as for different nations and regions the notion carries different prerequisites, context and practice.

There are famous examples of cyber threat hype coming from high-level politicians explaining the need for national attention towards cyber security, the most famous probably being that of "cyber Pearl Harbor": "Imagine a few years from now: A President goes forth and orders troops to move. The lights go out, the phones don't ring, the trains don't move. That's what we mean by an electronic Pearl Harbor."[37]

Others ask how to prevent "Cyber 9/11", drawing a parallel between the terrorist attacks of September 2011 and how we lead our life in the information society: „Today, in less than a lifetime, the Internet has become the most promising and ingenious communication tool in human history. At the same time, it's also become a gateway for attacks and crimes that are getting more frequent, damaging, and inventive. The stage is set for a whole new level of boldly conceived action – as it was in September 2001."[38]

Although dramatisation of the actual threat can be regarded as a valid and integral part of the securitisation process[39], in the cyber security context this has resulted in a confusion of responses and approaches.[40] Especially from the legal perspective, clarity in underlying concepts and current definitions is essential in

---

Publishers, Boston, 2006. Available at http://faculty.nps.edu/dedennin/publications/Cyberterror%202006.pdf (last accessed May 5, 2011).

[32] Vineetha Menon. FBI: Cyber terrorism threat is 'rapidly expanding'. Available at http://www.itp.net/579523-fbi-cyber-terrorism-threat-is-rapidly-expanding (last accessed May 5, 2011).

[33] Dorothy E. Denning. Cyberterrorism – Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives. 2000. Myriam Dunn Cavelty. Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. – Journal of Information Technology and Politics. Vol. 4, No. 1, 2007, pp. 19–36.

[34] For example international organisations like EU, G8, Council of Europe.

[35] *Supra nota* 28.

[36] See Anna-Maria Talihärm. Defining Cyberterrorism. – LLM thesis. Stockholm University, 2008.

[37] Tim Weiner. The Man Who Protects America from Terrorism. – New York Times, 1 February 1999, p. A3.

[38] Alan Drummer. Cyber 9/11. How Do We Prevent It? – Symantech CIO Online Digest Extra. November 2009. Available at http://eval.symantec.com/mktginfo/enterprise/ articles/b-ciodigest_october09_cyber_911.en-us.pdf (last accessed May 5, 2011).

[39] *Supra nota* 11, p. 6–7.

[40] A good example of this is the Estonian incident of 2007 that got referred to as "Cyber War I", "Cyber blockade" and "an event similar to a nuclear explosion" by politicians.

order to assess the legal framework applicable, remedies available and authorities responsible for handling the incidents. As observed by Ohm[41], fear often dominates debates about cyber conflict.

The cyber threat spectrum has expanded significantly after Estonia and Georgia became the first internationally discussed examples of nation-states experiencing cyber incidents affecting the functionality of national government[42]; since then countries like Russia and China have been publicly accused of launching national security relevant cyber attacks against numerous countries[43]. Recent international discussions have led to more determined steps towards re-shaping the national cyber security strategies and filling the gaps in laws that have allowed politically motivated cyber attacks to remain non-punishable – Estonia, Sweden, the UK and the The US are just a few examples of countries recently updating their strategic views on cyber security. A reflection of real-life cyber attacks can be seen in the increased attention to cyber security issues by most international organisations and a number of states – the adoption of NATO's Cyber Defense Policy[44] and Strategy[45] in 2008, the ITU Toolkit for Cybercrime Legislation[46], the EU Communication on Critical

---

[41] Paul Ohm. The Myth of the Superuser: Fear, Risk, and Harm Online. – University of Colorado Law School, 2007. Available at http://ssrn.com/abstract=967372 (last accessed May 5, 2011).

[42] Charles Clove. Kremlin-backed group behind Estonia cyber blitz. – Financial Times, 11 March 2009. Available at http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?nclick_check=1 (last accessed May 5, 2011). Robert Coalson. Behind The Estonia Cyberattacks. – RFE/RL, 6 March 2009. Available at http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html (last accessed May 5, 2011). Gadi Evron. Battling Botnets and Online Mobs. Estonia's Defense Efforts during the Internet War. – Georgetown Journal of International Affairs. Winter/Spring 2008, pp. 121-126; Mikko Hyppönen. Unrest in Estonia. 28 April 2007. Available at http://www.f-secure.com/weblog/archives/00001181.html (last accessed May 5, 2011). Mark Landler, John Markoff. In Estonia, what may be the first war in cyberspace. – International Herald Tribune. 28 May 2007. Available at http://www.iht.com/articles/2007/05/28/business/cyberwar.php (last accessed May 5, 2011). NATO Sees Recent Cyber Attacks on Estonia as Security Issue. – Deutsche Welle, 26 May 2007. Available at http://www.dw-world.de/dw/article/0,2144,2558579,00.html (last accessed May 5, 2011).

[43] See, e.g., Dan Goodin. India and Belgium decry Chinese cyber attacks. – The Register, 8 May 2008. Available at http://www.theregister.co.uk/2008/05/08/belgium_india_china_warnings; John Leyden. France blames China for hack attacks. – The Register, 12 September 2007. Available at http://www.theregister.co.uk/2007/09/12/french_ cyberattacks (last accessed May 5, 2011). Rhys Blakely, Jonathan Richards, James Rossiter and Richard Beeston. MI5 alert on China's cyberspace spy threat. – The Times, 1 December 2007. Available at http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece (last accessed May 5, 2011).

[44] NATO Cyber Defense Policy. 20 December 2007. Document with restricted access.

[45] NATO Cyber Defense Concept. 13 March 2008. Document with restricted access.

[46] ITU Toolkit for Cybercrime Legislation. February 2010. Available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf (last accessed May 5, 2011).

Information Infrastructure Protection[47] and proposed Directive on Attacks against Information Systems, repealing of the Council Framework Decision 2005/222/JHA, and the reopened discussions in the UN governmental experts' working group on information security[48] are just some examples of emphasis added to global cyber security.

To sum up, the task of reviewing and adjusting the existing remedies is not new to the international community. Lessons learned from cyber incidents brought the international community to an understanding more than a decade ago that collective efforts are needed to counter cyber crime.[49] This time the challenge is even more complicated and requires the correction of previous errors along with building up a coordinated approach to global cyber security.

1.1. Information Society as a Dimension of Life and Law

These days one can refer to the information society as *res ipsa loquitur*, considering how information and communication technology has influenced the world's way of life, forming an integral part of international and regional development agendas and being a means easily accessible and familiar to millions of people all around the globe regardless of age and ethnicity. A number of articles and papers have been written to describe this emerging reality[50] and influential international[51] instruments have explained how this term is to be understood. Nations have developed their approaches in more detail:

> "The European process of development is clearly progressing towards a knowledge-based (new) economy and information society. If we are not properly

[47] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM (2009) 149).

[48] The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security presented a report to the Secretary-General by the end of 2010.

[49] Council of Europe Convention on Cybercrime. Budapest, 23.XI.2001.

[50] E.g. Manuel Castells. The Information Age. Economy, Society, and Culture. Vol. 1–3. – Wiley-Blackwell, 2010; George Orwell. 1984. – London: Secker & Warburg, 1949.

[51] E.g. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime (COM (2000) 890). Available at http://www.justice.gov/ criminal/ cybercrime/intl/EUCommunication.0101.pdf (last accessed May 5, 2011). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), 17.7.2000 EN L 178/1 Official Journal of the European Union. OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam, 2006. Available at http://www.oecd.org/dataoecd/43/28/ 38770483.pdf (last accessed May 5, 2011).

> prepared and remain merely passive observers or only follow the changes which will occur from a distance, we shall benefit less from the process. Our disadvantage will, sooner or later, turn into dependence, or, in a worst case scenario, into a subordinate status. Reducing our shortfall is in our common interest: enhancing the competitiveness of the economy will lead to an improvement in the quality of life in Hungary, while for the community as a whole it will improve the competitive status of the European region in relation to the North American and Far East regions."[52]
>
> "The information society vision of Turkey and of the Turkish Government is not only to become a society using technology, but also to create an asset for both her citizens and for all humanity, and to make new and solid contributions to accumulation of universal civilisation. We believe that in order not to lag behind with regard to information society and in order to avoid exposure to unfair competition in all areas, we have to renew and develop ourselves and our institutions."[53]

While the analyses of various definitions concludes that 'information society' is a statement of a global trend towards more dependence on the use of information and communication technology, the level of information society development and the characteristics of information society significantly differ by countries and regions. Hirvonen and Frank explain that 'information society indicators' are used to describe the level of information society development achieved in a particular society.[54]

From the legal perspective, this understanding plays an important role in deciding what aspects of the information society are critical to secure and possibly regulate on a national level. For example, countries may have different priorities as regards the desired impact of e-commerce, the appropriate balance between privacy and freedom of information, or criminal policy in the field of cyber crime.

An understanding of the background and framework of the information society will allow one to determine the international consensus and obstacles to the cyber security debate – the concerns of Estonia could be similar to those of Latvia and Finland, but simply because of differences related to ICT infra-structure and information society maturity, they cannot coincide with those of the United States or Georgia.

It is therefore not the definition, but the perception of information society that varies significantly by nations and individuals and determines their

---

[52] Hungarian Information Society Strategy. – Informatikai és Hírközlési Minisztérium. Available at http://www.epractice.eu/files/media/media_308.pdf (last accessed May 5, 2011).

[53] Information Society Strategy and Annexed Action Plan. – State Planning Organisation. 2006. Available at http://www.bilgitoplumu.gov.tr/Documents/5/Documents/060700_InformationSocietyStrategy.pdf (last accessed May 5, 2011).

[54] Timo Hirvonen, Lauri Frank. Measuring the Information Society in Europe: From Definitions to Description. – ERSA conference papers, 2006. Available at http://ideas.repec.org/p/wiw/wiwrsa/ersa06p764.html (last accessed May 5, 2011).

approach to cyber security. From a terminology point of view, the notion of information society seems to be used consistently by nations and international organisations:

> "We, the representatives of the peoples of the world, assembled in Geneva from 10–12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to build a people-centered, inclusive and development-oriented Information Society, where everyone can create, access, utilise and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights."[55]
> "The information society is a comprehensive concept. It covers social reality in its totality. Development of information and communication technologies has changed, and is continuing to change today's world remarkably, even though we are not aware of all upcoming changes."[56]
> "Dmitry Medvedev approved a list of Presidential instructions following a joint meeting of the State Council and the Presidential Council for the Development of an Information Society in the Russian Federation on December 23, 2009."[57]

The content and context of these statements can only be understood after familiarizing oneself with the information society of the country or group of origin of the statement. For example, developing the information society in Russia these days means setting a common policy for electronic provision of services for all agencies and regions; developing the legal and regulatory framework in this area; reducing the digital gap between the different regions; and training qualified IT personnel for public sector and government institutions by 2015.[58] In Russia, 36% of inhabitants use the Internet[59] and Russia has the fastest growing Internet population in Europe, followed by France and Spain.[60]

---

[55] Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. – World Summit on the Information Society, 2003. Available at http://www.itu.int/wsis/docs/geneva/official/dop.html (last accessed May 5, 2011).
[56] *Supra nota* 27.
[57] Dmitry Medvedev approved a list of Presidential instructions following a joint meeting of the State Council and the Presidential Council for the Development of an Information Society in the Russian Federation. 30 December 2009. Available at http://eng.kremlin.ru/news/121 (last accessed May 5, 2011).
[58] Joint session of the State Council and the Presidential Council for the Development of an Information Society in the Russian Federation. 23 December 2009. Available at http://eng.kremlin.ru/news/122 (last accessed May 5, 2011).
[59] Number of Internet Users in Russia Increased by Over 20% in 2009. The School of Russian and Asian Studies, 20 January 2010. Available at http://www.sras.org/russian_internet_usage_increases (last accessed May 5, 2011).
[60] Erick Schonfeld. Russia Is Rising in Internet Population. TechCrunch, 27 August 2008. Available at http://www.techcrunch.com/2008/08/27/russia-rising-in-internet-population/ (last accessed May 5, 2011).

For Estonia, at the same time, the key challenges in developing the information society include integration of the public, private and third sector into one service space to improve the quality of service provision in the public sector; identification, development, and implementation of high impact services (e-Procurement, e-Invoicing etc.); development of public sector e-services in different fields of life for citizens, businesses and public sector agencies; and opening up of Estonian e-services for the citizens of other countries, especially those from the EU member states.[61] Currently, the Internet usage rate in Estonia is about 68%.

Thus, Estonia and Russia are neighbouring countries with rather different perceptions of the content and essential properties of the term "information society". Estonia shares the information society approach with other "virgin territories" for ICT development born after the Cold War. At the same time, not all 'dissolved' countries have followed a similar path when it comes to developing an information society agenda. There are countries where the Internet penetration is rather low (in Georgia 28,3%[62]) or growing rapidly and who therefore undergo a review of their earlier information society priorities (India, China[63]). And for a number of countries, for different reasons, the information society is just getting started – as part of the rule of law and organisational structure of a society that has been tackling more life-critical issues than IT infrastructure – or will start in the distant future.

Other factors that may influence national cyber security priorities include the reality of telecommunications capabilities (countries with "heritage" communication systems – most of Western Europe and US[64]; and countries with no effective telecommunications capability), information architecture and national priorities regarding the accessibility of common resources (restrictions to the use of the Internet by the public in North Korea and China[65]), as well as the availability of Internet resources (e.g. the shortage of IPv4 addresses[66]) in the first place.

It is therefore not only the statistical data[67] of Internet usage and the "internetisation" of the public and private sectors that will determine the nature of the

---

[61] *Supra nota* 27.

[62] Internet World Stats. Available at http://www.internetworldstats.com/stats3.htm#asia (last accessed May 5, 2011).

[63] Internet usage growth during the period of 2000-2010 has been 1520% in India and 1766,7% in China. – Internet World Stats. Available at http://www.internetworldstats.com/asia.htm#in (last accessed May 5, 2011).

[64] For example, Germany's broadband Internet market is heavily dominated by DSL.

[65] See, e.g., China Tightens Internet Restrictions. – Voice of America. 23 February 2010. Available at http://www1.voanews.com/english/news/asia/China-Tightens-Internet-Restrictions-85043447.html (last accessed May 5, 2011).

[66] David Meyer. IPv4 addresses: Less than 10pc still available. – ZDNet UK. 19 January 2010. Available at http://www.zdnet.co.uk/news/networking/2010/01/19/ipv4-addresses-less-than-10pc-still-available-39994507/ (last accessed May 5, 2011).

[67] It is important to note that the statistical reviews of information society development are based on different methodologies and resources and thus may vary significantly.

information society. Economic situation, geographical location, and size of territory and population, as well as geopolitical relations, all play a role when assessing an information society and determining the priority areas for development and defence.

1.2. The Challenging Nature of the Internet

For the purposes of this dissertation the information society as we know it started with the Internet, which in turn started with the ARPANET project back in the 60s. J.C.R. Licklider (1915–1990), under whose leadership the ARPANET project achieved a qualitative change, can be considered one of the spiritual fathers of the modern information society. Licklider thought it was essential to have people communicating with other people using computers; his approach differed somewhat from the initial emphasis on a computer communicating with another computer.[68]

Some argue that information society was born together with the printing art and that the challenges related to it are not much different from those we faced with the birth of telegraph.[69] For the purposes of further argumentation, the "new era" information society paradigm will be used as a point of departure.

The Internet was originally not meant for the public. It was designed for the (US) military. This, to an extent, explains why the United States have always been on the forefront of Internet related initiatives, be commercial, military or academic by nature. [70]

When looking at some of the essential legal issues surrounding the Internet these days, in the original context of the Internet many of them would not be problems at all. For example, anonymity was never really an issue when

[68] The two papers Licklider wrote on the concept of computers and communications: Joseph Licklider. Man-Computer Symbiosis. – IRE Transactions on Human Factors in Electronics. Volume HFE-1, March 1960, pp. 4–11; Joseph Licklider. The Computer as a Communication Device. – Science and Technology. April 1968. Both papers were reprinted by Digital Equipment Corporation in 1990 and are available at http://memex.org/licklider.pdf (last accessed May 5, 2011).

[69] Tom Standage. The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers. – Walker & Company 1998.

[70] In 1968 the US Department of Defense launched the project ARPANET (Advanced Research Projects Agency) with the goal to create data communications networks which could function even after having suffered partial damage (e.g. due to a bomb attack). That network employed sending messages in small packets that could be forwarded separately and via different routes. The second goal was to give scientists the possibility to connect with big remote computer-centres to use the hardware and software resources of mainframe computers (memory, databases and supercomputers' data processing capability); in that framework the first packet data network was created between four US universities. The project was mainly prompted by defense interests and the goal to create a functioning data communications network in case a Third World War broke out. See more in, e.g. Barry M. Leiner et al. A Brief History of the Internet. Available at http://www.isoc.org/internet-/history/brief.shtml (last accessed May 5, 2011).

developing the early concept of the Internet – with only defence and science networks connected, and the US Government in control of the reach of the network, the architecture of the network did not cause any such issues. Although the future uses of the Internet were perceived to be potentially wider than just defensive, those views did not prevail in the early stages of development of the Internet from the regulatory perspective. Regardless of where the information society began, it is observed that most of the challenges we face in cyber security started after opening the computer networks for public use, thereby rendering access to networks anonymous.[71]

As Dunn Cavelty explains, opening the Internet to public use changed the nature of the issues around the use of it – a criminal could alter data and programs from home, without physical entry into the victim's building.[72] Certain uses of computer networks have introduced new kinds of activities that affect personal, economic or social welfare and are potentially detrimental to the development of information society in general. Attached to it come the regulatory challenges described by Murray – the global reach of cyberspace allows people to evade state-based control by utilizing the network architecture, and the internal design aspect enables a unique level of environmental control through manipulation of the code.[73]

Although laws and regulations have accompanied the evolution of the Internet from the early stages, it has been very difficult to keep up with the development of the phenomenon. First, the rapid development of technology complicates the process of legislation.[74] As Goldman explains from a teacher's perspective: "Cyberlaw changes constantly. For example, during the 1990s, I routinely replaced one-third of my teaching materials every year; and I no longer teach any materials from my Spring 1996 course reader."[75] In a way, attempts to regulate the Internet could be compared to patching leaks in a cross-

[71] See, e.g., Marco Gercke. Europe's Legal Approaches to Cybercrime. – ERA Forum. Vol. 10, No. 3, 2009, p. 410.
[72] *Supra nota* 3, p. 46.
[73] Andrew D. Murray. The Regulation of Cyberspace: Control in the Online Environment. – Routledge-Cavendish, 2007, p. 34.
[74] The PC is just a bit less than 30 years old and the wireless technology was only invented about 15 years ago. Despite that, the speed of computers has increased 2600 times over 30 years. From just 100 Kb of storage capacity the external memory devices now can store up to several terabytes of data. The first commercial PC, the Altair 8800 (by MITS), used an Intel 8080 CPU with a clock rate of 2 MHz (2 million cycles per second). In 2002, an Intel Pentium 4 model was introduced as the first CPU with a clock rate of 3 GHz (3 billion cycles per second). The highest clock speed microprocessor ever sold commercially to date is found inside IBM's zEnterprise 196 mainframe, introduced in July, 2010. The z196's cores run continuously at 5.2 GHz. – Evan Selleck. IBM z196 5.2GHz CPU Breaks Records, Could Cost Hundreds of Thousands. – Slashgear, 25 August 2010. Available at http://www.slashgear.com/ibm-z196-5-2ghz-cpu-breaks-records-could-cost-hundreds-of-thousands-2599009/ (last accessed May 5, 2011).
[75] Eric Goldman. Teaching Cyberlaw. – Santa Clara University School of Law Legal Studies Research Papers Series. Paper No. 08-57, July 2008.

border water utility system without having a clear picture of the condition and architecture of the system on the other side. Its cross border nature and attribution are just a few examples of challenges to legal responses to cyber incidents these days.

Further obstacles to legislation and legal policy adjustments include the fact the society is changing along with the technology it adopts and that this change is not yet stabile – although a global phenomenon, the availability of the Internet and its importance from a national development point of view drastically differs by regions.

Also, attempts to regulate the Internet and information society's behaviour have been condemned by the community of users as well as criticised by technology experts.[76]

Fourthly, circumstances and priorities also change over time – as judge Schjølberg notes, the Convention of Cybercrime, the main document for countries to align their cyber security, criminal law and policy with, is based on the criminal conducts of the late 1990s and does not cover new methods of conduct such as phishing, botnets, spam, cyber terrorism and massive and coordinated attacks against information infrastructures. /…/ In addition, the terminology included in the Convention is a 1990s terminology, and is not necessarily suitable for 2010s.[77] Even Sieber's argument about the "broad" wording of the convention does not resolve the issues related to uniform application.[78]

In short, as the technology develops and the society adopts it, the challenges for regulation change – as do priorities for legal policy. For example, the principle of neutrality of Internet Service Providers (ISP) has developed extensively over the past two decades. At the early stages of the Internet, ISP liability was not regulated. In 1996 the US Congress exempted ISPs from liability for unlawful or tortious acts committed over the Internet unless they were directly involved in the activity.[79]For the purposes of the development of the Internet, the Communications Decency Act stated the policy of the United States a) to promote the continued development of the Internet and other interactive computer services and other interactive media; b) to preserve the vibrant and competitive free market /.../; c) to encourage the development of technologies which maximise user control /.../; d) to remove disincentives for the development and utilisation of blocking and filtering technologies [for parental control] and e) to ensure vigorous enforcement of Federal criminal

[76] See, e.g., John Perry Barlow. A Declaration of the Independence in Cyberspace. 8 February 1996. Available at http://homes.eff.org/~barlow/Declaration-Final.html (last accessed May 5, 2011).
[77] *Supra nota* 16, p. ii.
[78] Ulrich Sieber et al. Cyberterrorism – the Use of the Internet for Terrorist Purposes. – Council of Europe Publishing, 2007.
[79] Roy J. Girasa. Cyberlaw: National and International Perspectives. – Prentice Hall, 2002, p. 103.

laws /.../.[80] The Congress compared ISPs to postal or express-mail deliverers who merely convey to receivers what was given to them by senders of the letters or packages. Just as mail carriers are not responsible for the content of the material delivered, ISPs have similar exemption from responsibility unless they directly engage in tortious or criminal conduct.[81]

A similar approach has been taken by European countries. Under the e-Commerce Directive[82] adopted in 2001, an ISPs liability for the activities on the network correlates to the business incentives and the ISP's direct involvement in any particular activity.[83]

There are considerable concerns about the effects of this approach under the current cyber security paradigm. Lichtman, Posner and others suggest that ISPs need to be brought into the chain of responsibility as they are in a good position to reduce the number and severity of malevolent acts online.[84] With more and more governments concerned with cyber attacks against national critical information infrastructures, a new ISP involvement policy is a considerable alternative to the efforts to impose security on the end-user level.

Examples of imposing additional obligations on the market are known from the past. At the stage of early development of phone services, the US government's policy towards a major telecommunications service provider, AT&T, favoured a monopoly as the primary purpose was to promote standardised services and the availability of services. Years later, when the market had matured, AT&T was carved up in order to promote diversity and availability beyond one market player's capability. Today, as Posner points out, ISPs are the key stakeholders in Internet communications.[85] For security purposes, their exact role and responsibility as part of communication infra-structure could be reconsidered as one of the effective ways to exercise more effective control over cyberspace.

Recently, attempts have been made to re-engage communication service providers in roles supporting law enforcement and other national authorities in securing cyberspace. An example in the EU context would be the Data Retention Directive[86] adopted in 2006. Pursuant to this instrument, Member States were required to make available for the purpose of the investigation, detection and prosecution of serious crimes, data regarding the traffic and

[80] *Ibid.*
[81] *Ibid*, p. 104.
[82] E-Commerce Directive (s*upra nota* 51).
[83] E-Commerce Directive (*supra nota* 51), Articles 12–15.
[84] Erik P. Posner, Douglas Lichtman. Holding Internet Service Providers Accountable. – Mark F. Grady, Francesco Parisi (Eds.). The Law and Economics of Cybersecurity. New York: Cambridge University Press, 2006, pp. 222–223.
[85] *Ibid*, p. 223.
[86] Directive 2006/24/EC 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. (Data Retention Directive).

location of communications.[87] The requirement to retain data extends to data generated or processed by providers of publicly available electronic communications services or of a public communications network.[88] The implementation of the Directive required Member States to specify the details of making data retained available to the competent authorities without undue delay upon request.[89] This involved negotiations between the authorities and the private sector on the investments and effort in making such data available and in most cases resulted in additional obligations to communications service providers as regards the availability of data identifying the source, destination, type, duration, equipment and location of the communication.[90]

Other recent examples of the changing way of online life include attempts to resolve the issue of limited IP addresses and employ another 340 trillion IP addresses under the new IPv6 standard.[91] Also, ICANN has introduced Domain Name System Security Extensions (DNSSEC)[92] project to increase transparency of Internet traffic allowing Internet users to know with certainty that they have been directed to the website they intended and thereby reducing fraudulent behaviour in the Internet.

These are only a few examples of on-going efforts to secure the activities online. Along with every new technology and security solution the cyber security picture will change slightly and the means and methods of security need to be adjusted to the threat picture and tools available.

1.3. The Information Community

To understand the impact of users on information society development, a brief look at statistics would be useful. By 1990, the Internet was used by 3 million people of whom 73% were living in the United States and 15% in Western Europe. Outside Western Europe and the United States, most users lived in Canada, followed by Australia, then Japan, the Republic of Korea and Israel.[93] In 2000, the total number of Internet users was about 360 million, about 25% of the users coming from Asia. By 2011, the total number of Internet users in the World had reached 2 billion, which is 1/3 of the global population. According to statistics, over 40% of Internet users are from Asia, 24% from Europe and 14%

[87] *Ibid*, Article 1 (1).
[88] *Ibid*, Article 3 (1).
[89] *Ibid*, Article 8.
[90] *Ibid*, Article 5.
[91] See, e.g. David Carr. Five Things You Need To Know About IPv6. – Computerworld, August 31, 2010.
[92] See Press Release at http://www.prweb.com/releases/DNSSEC/Cyber_Crime/prweb4321774.htm.
[93] Internet Users 1990. Worldmapper. Available at http://www.worldmapper.org/display.php?selected=335 (last accessed May 5, 2011).

from North America.[94] For millions of people, information society is no longer a revolution but reality – a dimension of their life in which they study, communicate, trade and date.

It is therefore not difficult to understand why the popularisation of the Internet has driven the regulatory efforts initially towards consumer protection, convenience of online transactions and a catalogue of redesigned rights and freedoms. On the other hand, this understanding should also alert the legislature to the difficulties of attempting to restrict and shape users' behaviour on the Internet. Even though possibilities exist to make mandatory security measures be adopted by home users, the number of users as well the architecture of the Internet make it difficult to enforce such regulations and thus would dilute the already weak authority of law. In a sense, the governments have over time lost the position to directly address and engage the end users. Instead, regulation needs to focus primarily on the stakeholders over whom governments still can exercise effective control and who, in turn, may be able to gradually influence the habits and culture of the online community.

The community of individual users has attracted commerce and industry stakeholders – and another regulatory concern arises from the contradiction of business and national security interests. Internet and communication service providers have enjoyed a power-user role in developing the information society as we know it and often have business interests that would be affected by potential security restrictions. In 2007, a conservative estimate of annual revenue for the top 99 Social Computing application provider companies, which employ between 7,000–8,000 people, was 3 billion USD (including also advertising revenues).[95] Market analysts forecast that world revenues will grow from about EUR 1 billion in 2008 to EUR 7–8 billion in 2013 when the market segment of mobile content and applications will be third, after music and gaming.[96]

These numbers are hard to overestimate, as is the impact of the user community on the development of the information society. The European Commission observes the impact of social computing[97] on the EU information society and economy, explaining how the market-oriented approach to information society development has resulted in not only the largest marketplace in the world, but also a global community of users. Without general awareness,

---

[94] Internet Usage Statistics. Internet World Stats. Available at http://www.internetworldstats.com/stats.htm (last accessed May 5, 2011).

[95] Kirsti Ala-Mutka et al. The Impact of Social Computing on the EU Information Society and Economy. – Institute of Prospective Technological Studies, European Commission. 2009, p. 18. Available at http://ftp.jrc.es/EURdoc/JRC54327.pdf (last accessed May 5, 2011). The report also explains that 3 billion USD corresponds to roughly 0.1% of the total revenues in the ICT sector, and the number of employees corresponds to an even lower share.

[96] *Ibid*, p. 18.

[97] *Ibid*, p. 15.The Report defines Social Computing as a set of open, web-based and user-friendly applications that enable users to network, share data, collaborate and co-produce content.

understanding and acceptance of contemporary cyber security risks, the community of users will pose a significant risk to national security efforts.

Another aspect of the online community relevant to cyber security is that virtually every computer owner can become a target or perpetrator of a cyber attack. It has been suggested that cyber threats are increasing because it is cheap and easy to launch cyber attacks instead of engaging in "physical" conflicts.[98] Denning doubts, however, if the barriers to entry are really lower in cyberspace than in the physical domain of warfare and suggests that the fact that cyber attacks seem to have a lower barrier to entry is because they are so commonplace.[99]

In sum, the role of the Internet user community in both the threat and security solutions is hard to overestimate. Yet only a few best practices exist on successfully engaging private users in wide-reaching cyber security solutions. Thus, addressing and engaging the community of users is currently out of reach as an immediate security-enhancing feature for most national governments.

1.4. The Contemporary Concept of Cyber Security

The Information Age and Society are characterised as a new social reality and a new global commonality.[100] Trying to define the security aspect of it is complicated first by the lack of a widely accepted definition of the information society itself. Often, the prefix "cyber" is used to describe the scope and extent of the emerging security concerns. As explained above, there are slightly different approaches to this term from legal, policy and technology points of view.

The term "cyber security" has been developed and cultivated primarily by the policy community. Schachtman explains:

> In Washington, "cybersecurity" is a term that's come to have a thousand meanings, and none at all. Any crime, prank, intelligence operation, or foreign-government attack involving a computer has become a "cyber threat." But at the Pentagon, they aren't worried about some kid painting a Hitler moustache on Defense Secretary Robert Gates' online portrait. They're not even that concerned about a full-scale attack on the military's networks – even though the modern American way of war depends so heavily on the free flow of data. In the military, there's now broad agreement that one cyber threat trumps all others: electronic

[98] See, e.g. Rain Ottis. From Pitchforks to Laptops: Volunteers in Cyber Conflicts. – Conference on Cyber Conflict Proceedings 2010, C. Czosseck and K. Podins (Eds.). CCD COE Publications, 2010, Tallinn, Estonia.

[99] Dorothy E. Denning. Barriers to Entry: Are They Lower for Cyber Warfare? – IO Journal, April 2009.

[100] See, e.g., Stine Gotved. Time and space in cyber social reality. – New Media Society. Vol. 8, No. 3, June 2006, pp. 467-486. Stein Schjolberg. A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime. – United Nations, 2010.

> espionage, the infiltration (and possible corruption) of Defense Department networks.[101]

By "Washington" and "Pentagon", Schachtman primarily refers to policy-makers involved in cyber security critical thinking either from the governmental or military perspectives. Recently, the term "cyber security" has widely been used in policy and strategy documents, sometimes left undefined, contributing towards a "popular term of art"[102, 103].

From the US perspective, popular sources explain cyber security as "the protection of data and systems in networks that are connected to the Internet"[104], but also refer to "information security"[105], a term frequently used by experts. According to the US National institute for Standards and Technology (NIST), information security is to be understood as "the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability"[106].

NIST goes on, explaining "1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; 2) confidentiality, which means preserving authorised restrictions on access and disclosure, including means for

---

[101] Noah Schachtman. Cybersecurity: Here's What Really Worries the Pentagon. Available at http://www.wired.com/dangerroom/2010/01/cybersecurity-heres-what-really-worries-the-pentagon/ (last accessed May 5, 2011).

[102] The Estonian Cyber Security Strategy states: "National cyber security is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's interests and wellbeing." – Cyber Security Strategy. – Ministry of Defense, 2008, p. 7. Available at http://mod.gov.ee/files/-kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (last accessed May 5, 2011).

[103] Cyber Security Strategy of the United Kingdom defines cyber security as: "Cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers." Cyber Security Strategy of the United Kingdom. 2009, p. 9. Available at http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf (last accessed May 5, 2011).

[104] PCMAG Encyclopedia. Available at http://www.pcmag.com/encyclopedia_term/0,2542,t=cybers-ecurity&i=40643,00.asp (last accessed May 5, 2011). Also, Merriam-Webster Dictionary defines cybersecurity as "measures taken to protect a computer or computer system (as on the Internet) against unauthorised access or attack". Available at http://www.merriam-webster.com/dictionary/cybersecurity (last accessed May 5, 2011).

[105] US Government Information Exchange Glossary defines information security as "the protection of information against unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional". Available at http://www.ssa.gov/gix/definitions.html (last accessed May 5, 2011).

[106] Richard Kissel. Glossary of Key Information Security Terms. – National Institute of Standards and Technology. 2006, p. 40. Available at http://csrc.nist.gov/publications/nistir/NISTIR7298_Glossary_Key_Infor_-Security_Terms.pdf (last accessed May 5, 2011).

protecting personal privacy and proprietary information; and 3) availability, which means ensuring timely and reliable access to and use of information".[107]

The term "cyber security" is more frequently used in United States (US) legislation (e.g. the Cyber Security Enhancement Act of 2002[108], the Cyber Security Information Act of 2000[109]). The term has also been adopted by NATO in its policy documents[110]. At the same time, the EU mostly refers to terms such as network and information security (NIS)[111], information and communication technology (ICT) security, information technology (IT) security, information security, network security, etc.

The somewhat inconsistent use of terms in addressing security problems within the domain of the information society reflects the lack of a common framework directive from NIS in Europe. Instead, in the face of increasingly converging networks, the EU prefers to regulate security issues separately, but in a coordinated manner, within each sector of the Information Society.

The EU regards information security as the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems. [112]

While there are slight technical details that make these definitions slightly different in terms of their coverage, the key elements of confidentiality, integrity and availability are present in most concepts and thereby represent the core of cyber security from the technical perspective.

From the UK policy perspective, cyber security embraces both the protection of UK interests in cyber space, and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers.[113]

From the legal perspective, the broad definition of cyber security could potentially affect almost every area of Information Society and therefore every area of law as well. For example, EUR-LEX lists over 200 legal instruments related to information technology, telecommunications and data processing[114].

---

[107] *Ibid*.

[108] http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm (last accessed May 5, 2011).

[109] http://www.fas.org/sgp/congress/2000/cybersec.html (last accessed May 5, 2011).

[110] *Supra nota* 44, 45.

[111] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach (COM (2001) 298). It defines NIS as ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

[112] *Ibid*.

[113] *Supra nota* 103.

[114] List of legal acts available at http://eur-lex.europa.eu/en/legis/20101101/chap1320.htm (last accessed May 5, 2011).

Under Estonian law, 377 legal instruments regulate the administration of information systems and 885 provide guidance for processing of information, but only one contains the wording "cyber security".[115]

In a recent study requested by the European Parliament's Committee on Foreign Affairs, cyber security has been defined as 'security within, and from cyber-space'. Paul Cornish refers to cyber security as a 'broader problem for individuals, businesses, public and private organisations, governments and international organisations' than data theft or cyber espionage. He lists hacking, serious and organised crime; ideological and political extremism; and state-sponsored cyber-attacks as the key threats facing the EU.[116]

While most of the "original concept" of cyber security has been drafted having the private sector business and information society freedoms in mind, the concerns that reach the threshold of critical infrastructure protection and military information management often cannot be satisfied by using the priorities and tools of the former. For example, the priorities of confidentiality, integrity and availability are fundamentally different in the case of industrial control systems compared to business information systems and services.[117] There are only a few legal instruments drafted with these threats in mind.[118]

When it comes to information technology glossaries, "cyber security" is not necessarily a defined term at all. The US National Information Assurance Glossary[119] does not contain the definition. Instead, it refers to "computer security" – measures and controls that ensure the confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated[120]; and "information

---

[115] http://www.riigiteataja.ee (last accessed May 5, 2011).

[116] Paul Cornish. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. – Directorate-General For External Policies Of The Union, European Parliament. 2009, p. 6. Available at http://www.euro-parl.europa.eu/activities/committees/studies.do?language=EN. (last accessed May 5, 2011).

[117] Joe Weiss. The Need for Interdisciplinary Programs for Cyber Security of Industrial Control Systems. —WorldComp, 2010.

[118] E.g., Section 237(1) of the Estonian Penal Code: Acts of Terrorism – 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 or interference with computer data or hindrance of operation of computer systems as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population is punishable by five to twenty years' imprisonment, or life imprisonment. – Karistusseadustik. 6. juuni 2001. – RT I 2001, 61, 364; RT I, 12.11.2010, 1.

[119] National Information Assurance (IA) Glossary. – Committee on National Security Systems. 2010. Available at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf (last accessed May 5, 2011).

[120] *Ibid*, p. 15.

systems security" – protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users, including those measures necessary to detect, document, and counter such threats [121]. As Professor Julie Ryan explains, cyber security was developed as a concept in the 1960s, when it wasn't called cyber security – it was called computer security.[122] This indicates that for computer security communities, the national security dimension of their field is not a self-evident feature.

Cyber security can be regarded as the sustainability of nationally relevant information resources while to the extent possible supporting the advancement of information society goals in general. As will be explained later, cyber security encompasses a wide range of threats and remedies involving different authorities and areas of law. An understanding therefore is necessary about the specific concerns and aims when addressing the body of cyber security or any portion thereof.

1.5. Growth of Politically Motivated Cyber Attacks

Although politically motivated cyber attacks had occurred before 2007, international attention was drawn to the changing cyber security paradigm only after 2007 when Estonian governmental and private information systems were targeted by a cyber attack campaign lasting for more than three weeks. The attacks were a response to the Estonian Government's decision to relocate a Soviet World War II monument from the center of the Estonian capital to a military cemetery. The decision received heavy criticism from Russian authorities and the ethnic Russian minority in Estonia. The campaign of distributed denial-of-service attacks [123], defacement [124], spam [125] and online calls and instructions to attack servers was presumably launched by ethnic Russian activists.[126] The attacks crippled governmental communications, online media and electronic bank transactions and were seen to be endangering national security.

In the summer of 2008, the decision of the Lithuanian legislature to ban the use of Soviet symbols provoked a defacement attack on more than 300 Lithuanian websites.

---

[121] *Ibid*, p. 37.
[122] *Supra nota* 13.
[123] A concerted malevolent effort to deny access to any electronic device, computer, server, network or Internet resource by its intended users (*Supra nota* 17, p. 112).
[124] Arbitrarily replacing the content of a web site.
[125] Unwanted e-mail messages.
[126] See more in Peeter Lorents, Rain Ottis, Raul Rikk. Cyber Society and Cooperative Cyber Defense. In: Proceedings of HCI (14). 2009, 180-186. Also, *supra nota* 8.

The beginning of the Russo-Georgian War in August 2008 was accompanied by distributed denial-of-service attacks against Georgian authorities' web servers, and defacement of Georgian public websites.

In late the fall of 2008 and spring of 2009 a number of countries discovered a worm in their strategic communication systems. This malware, called Conficker, represented a type of software specifically designed to spread and compromise as many machines as possible, to set up, deploy and maintain a viable stealth communication system between the compromised machines for updating and command purposes, and to paralyze defensive systems, thereby creating a worldwide army of dormant machines, able to communicate, update and receive orders, while also neutralizing any defence system in place.[127]

In 2009, the elections on Iranian web sites were knocked off-line by an ad-hoc cyber protest against the results of recent Iranian elections.[128]

More recent cases such as Aurora (the 2010 attacks against Google and other corporations in China) and Stuxnet (a worm targeting the Iranian nuclear programme) show that cyber threats continue to increase in sophistication and scale.

1.6. International Cyber Security Interest Statements

An important outcome of the Estonian incident is the attention that several international organisations have paid to the topic in the past three years. NATO was one of the first to announce a cyber defence policy package in 2008 in response to cyber attacks against Estonia.[129] Although NATO had weighed cyber security concerns already in the 2002 Prague Summit, no urgent and systematic attention had been paid to the topic between 2002 and 2006. The EU has introduced a number of amendments to its cyber legal and policy framework originally dating back to the early 90s, and has adopted more since 2007[130]. In 2009, the UN opened discussions on cyber security by forming the

[127] BitDefender. Conficker – One Year After. White Paper (2010). Available at http://www.bitdefender.com/fi-les/Main/file/Conficker_-_One_Year_After_-_Whitepaper.pdf (last accessed May 5, 2011).

[128] Robert McMillan. With unrest in Iran, cyber-attacks begin. NetworkWorld, June 15, 2009. http://www.network-world.com/news/2009/061609-with-unrest-in-iran-cyber-attacks.html (last accessed May 5, 2011).

[129] NATO Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. Para 47. Available: http://www.summit-bucharest.ro/en/doc_201.html (last accessed May 5, 2011).

[130] E.g. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Also Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

Group of Governmental Experts on Information Security[131] and recently OSCE has redefined the need for a comprehensive approach to cyber security[132]. The cyber security agenda of international organisations has been provided in more detail in an article underlying this dissertation.[133]

1.6.1. NATO

NATO's cyber security concerns started as an element of mission security in the Kosovo crisis.[134] In 2002, NATO leaders at the Prague Summit decided that the organisation needed to defended against cyber attacks[135] and directed that a technical NATO Cyber Defence Programme be implemented, establishing the NATO Computer Incident Response Capability (NCIRC).[136]

The Istanbul Summit in 2004 did not address cyber security as a separate topic; but from Riga in 2006, the heads of states sent a broader message for securing the cyber side of NATO's mission:

> The adaptation of our forces must continue. We have endorsed /…/ work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber attack.[137]

Par. 47 of the 2008 Bucharest Summit Leaders' Declaration, obviously inspired by the cyber events in Estonia in 2007, stated a much more determined approach to cyber security:

---

[131] The work of this group resulted in the Note by Secretary General "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (A/65/201), 30 July 2010.

[132] OSCE Decision no. 991 OSCE conference on a comprehensive approach to cyber security: exploring the future OSCE role. PC.DEC/991, 31 March 2011.

[133] Eneken Tikk. Global Cyber Security – Thinking About Ways Ahead for NATO. – SAIS Review of International Affairs, Volume 30, Number 2, Summer-Fall 2010, pp. 105-119.

[134] For more details, see, e.g., Kenneth Geers. Cyberspace and the Changing Nature of Warfare. SCMagazine, 27 August 2008. Available at http://www.scmagazineus.com/cyberspace-and-the-changing-nature-of-warfare/ar-ticle/115929/ (last accessed May 5, 2011). See also *supra nota* 11, p. 5.

[135] Article 4 (f) of NATO Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002. Available at http://www.nato.int/docu/pr/2002/p02-127e.htm (last accessed May 5, 2011).

[136] Sverre Myrli. Report "173 DSCFC 09 E bis – NATO and Cyber Defense" of 2009 Annual Session. Available at http://www.nato-pa.int/default.Asp?SHORTCUT=1782 (last accessed May 5, 2011). Para 45.

[137] NATO Riga Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006. Available at http://www.nato.int/docu/pr/2006/p06-150e.htm (last accessed May 5, 2011). Para 23.

> NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defense, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defense emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defense capabilities and strengthening the linkages between NATO and national authorities.[138]

While the details of NATO's Cyber Security Concept have not been released to the public, one can conclude from these high-level policy documents in combination with a few publicly available presentations and press releases that from the initial mission security-focused and inward-directed defence of information systems against cyber attacks, NATO has developed a wide-reaching cyber security agenda covering assistance to Allies and strengthening cyber security-related cooperation between NATO and national authorities.

This agenda remains tied to NATO's overall goals and mission that will determine the focus of cyber security cooperation between the Allies who have decided to unite their efforts for collective defence and for the preservation of peace and security.[139] The collective defence commitment in Article 5 of the North Atlantic Treaty is not the only factor in NATO's approach to cyber security. For the purposes of Article 5, one could conclude that the main responsibility for NATO would be to define a "cyber armed attack" and provide the means for "cyber force" but this has not proven to be the main challenge for the organisation. While it is the natural course of action that over time NATO will develop internal procedures for implementing Article 5 in case of a cyber attack, currently the organisation's focus on cyber security inclines toward the procedures available under Article 4 of the North Atlantic Treaty[140].

Myrli observes that 'the report [*on cyber attacks against Estonia*] called for the development of a NATO cyber defense policy – a policy approved in January 2008, and endorsed by heads of state and government at the Bucharest Summit that April. The speed with which the NATO Policy on Cyber Defense was agreed highlights the very broad political consensus amongst Alliance Members as to both the seriousness of cyber threats, and NATO's potentially valuable role in this area. The Alliance's relevant military and technical bodies are currently engaged in implementing the policy, as are as the individual Allies'.[141] Myrli's conclusions are consistent with the information provided on NATO's official website:

---

[138] *Supra nota* 147.
[139] Preamble of the North Atlantic Treaty. Washington D.C., 4 April 1949. Available at http://www.nato.int/c-ps/en/natolive/official_texts_17120.htm (last accessed May 5, 2011).
[140] *Ibid*, Article 4, the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.
[141] *Supra nota* 136, para. 4.

> A major cyber attack on Estonian public and private institutions in April and May 2007 prompted NATO to take a harder look at its cyber defenses. At their meeting on 14 June 2007 Allied Defense Ministers agreed that urgent work was needed in this area.[142]

Myrli also reports that 'NATO dispatched *ad hoc* [rapid reaction] teams (RRTs) to Estonia and Georgia following the attacks in those countries in 2007 and 2008', and that 'new RRTs will be on call and available for immediate deployment should a member country make a political-level request to the Alliance. /…/ scheduled to be fully operational by 2012, the RRTs will consist of a combination of NATO members of staff and experts from member nations. If called into action, the RRTs will work under the direct guidance of the attacked nation.'[143]

Recent briefings by high-level officials also support the assertion that NATO's cyber security agenda has been shaped by the events of Estonia and Georgia.[144] However, the nature of these incidents is not directly relevant to Article 5 discussions as it remains below the threshold of "armed attack".[145] In the Estonian case the attacks never reached the threshold of an armed attack and in the Georgian case, although the cyber incidents occurred during a declared state of war between Georgia and Russia, neither of the nations involved was a full member of NATO.

In May 2010 the expert group led by Mrs. Madeleine Albright delivered its analysis and recommendations to NATO's Secretary General to assist him in drafting the new Strategic Concept.[146] The Group of Experts emphasises the significance of cyber threats and concludes that 'serious gaps' persist in NATO's cyber defence capabilities. Accordingly, the experts recommend that NATO recognises cyber attacks as a growing threat to the security of the Alliance and its members, and accelerates its responsive efforts by protecting NATO's communications and command systems and by helping Allies to improve their ability to prevent and recover from attacks. The group also recommends the development of an array of cyber defence capabilities aimed at effective detection and deterrence.[147]

---

[142] Defending against cyber attacks. – NATO Official Website. Available at http://www.nato.int/issues/-cyber_defense/index.html (last accessed May 5, 2011).
[143] *Supra nota* 136, para. 49.
[144] A brief by MG Koen Gijsbers to HRCSAC lists Kosovo War (1999-2000), US P-3 Incident with China (2001), Israeli-Lebanon War (2006), Estonian Cyber Conflict (2007), Georgian War (2008), India and Pakistan (continuous) and targeted trojans against NATO as examples of cyber security incidents requiring the organisation's attention.
[145] *Supra nota* 17, pp. 14-35; 66-90.
[146] NATO 2020: Assured Security; Dynamic Engagement. 17 May 2010. Available at http://www.nato.int/c-ps/en/natolive/official_texts_63654.htm (last accessed May 5, 2011).
[147] *Ibid*.

The Lisbon Summit in November 2010 set the goal of introducing a revised cyber defence policy and action plan by June 2011. On June 8, the following press statement was made:

> "The revised policy will offer a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber threats and building resilience. All NATO structures will be brought under centralised protection, and new cyber defence requirements will be applied. The policy clarifies political and operational mechanisms of NATO's response to cyber attacks, and integrates cyber defence into NATO's Defence Planning Process. The policy also sets the principles on NATO's cyber defence cooperation with partner countries, international organisations, the private sector and academia."[148]

These developments make NATO a new and important player in the global cyber security arena. Unlike many other international organisations, NATO has no comprehensive legacy that would pre-define its approaches to global cyber security.[149] It's focus is pre-defined with its mandate of national and international peace and security, thus balancing against other organisations' focus areas and initiatives.

1.6.2. EU

The EU got involved in regulation of electronic commerce in the late 1980s. The foundations of Community activity in this respect were laid in 1987 with the establishment of the Electronic Data Interchange (EDI) programme which had the objective of encouraging the use of EDI in trade. For more than 10 years the cyber security concerns of the EU focused on establishing user trust in the digital environment and had the aim to 'create a clear and stable legal framework at Community level in order to foster the development of the Information Society'[150]. The original areas of EU attention included taxation, electronic signatures, copyright, data protection, commercial communications, consumer protection, distance contracts and other aspects of electronic commerce.[151]

In the late 90s cybercrime was added to the EU's topics of interest. In April 1998, the Commission presented to the Council the results of a study on computer-related crime (the so-called 'COMCRIME' study). In October 1999, the Tampere Summit of the European Council concluded that the consideration

---

[148] http://www.nato.int/cps/en/natolive/news_75195.htm. (last accessed June 25, 2011).

[149] For further discussion on NATO's role and niche in the global cyber security model, see *supra nota* 133.

[150] Directive 98/48/EC of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. OJ L 217/18 05.08.1998. Recital 6.

[151] For an overview of the EU early approaches to cyber security, see John Dickie. Internet and Electronic Commerce in the European Union. – Oxford, Portland Oregon: Hart Publishing, 1999.

of high-tech crime should be included in the efforts to agree on common definitions and sanctions.[152] In the COMCRIME study, Professor Ulrich Sieber concluded: "Deficits of clearly defined European solutions exist especially with respect to non-legal measures as well as with respect to economic criminal law, illegal and harmful contents, criminal procedural law, security law as well as the sanctions in the field of data protection law."[153] Sieber pointed out the following priority actions:

– creating minimum rules of criminal law for fighting international computer crime, especially in international computer networks, including the coordination of accepted standards for contents,
– recommending adequate coercive powers (including solutions for encrypted data) with respect to the investigations of computer crime in international computer networks,
– dealing specifically with trans-border investigations involving international computer networks (e.g. freezing operations),
– solving conflicts of jurisdictions arising from international computer networks (especially with respect to illegal contents which could fall under a multitude of jurisdictions).[154]

Sieber also suggested that the Council should have the competence to deal with the above-mentioned legal problems in joint actions (or, after the ratification of the Amsterdam Treaty, in framework decisions) and in conventions. Considering the time required for the ratification of conventions, he recommended using – at least as a first approach – the instruments of joint actions or framework decisions.[155]

In 1999, the European Parliament and the Council adopted a Multiannual Community Action Plan promoting safer use of the Internet by combating illegal and harmful content on global networks[156], which was followed by several documents on improving the security of information infrastructure[157].

It can be argued that until now, the 2005 Council Framework Decision on attacks against information systems[158] is the most important EU anti-cybercrime activity since it aims to improve cooperation between the judiciary and other

[152] *Supra nota* 51, p. 2.
[153] Ulrich Sieber. Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study. —University of Würzburg, 1998, p. 6.
[154] *Ibid*, p. 238.
[155] *Ibid*, p. 237.
[156] Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999D0276-:EN:HTML
(last accessed May 5, 2011).
[157] *Supra nota* 153, pp. 56-78.
[158] Council Framework Decision 2005/222/JHA of 17 January 2005 on attacks against information systems, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT
(last accessed May 5, 2011).

competent authorities, including the police and other specialised Member States law enforcement services. The Framework Decision aims to reach its objectives by approximating rules on criminal law in the Member States in the area of attacks against information systems[159] by defining such criminal attacks against information systems as piracy, viruses and denial of service attacks. More importantly, the document underlines the importance of approximation of criminal law systems and the enhancement of cooperation between judicial authorities concerning illegal access to information systems, illegal system interference and illegal data interference. The Member States will have to make provisions for such offences to be punished by effective, proportionate and dissuasive criminal penalties. In 2010, a Proposal for a Directive on attacks against information systems[160], repealing Framework Decision 2005/222/JHA, was made that is currently work in progress.

In addition to the Framework Decision, the European Commission has addressed the cyber crime issue in more detail in the 2007 Communication on "Towards a general policy on the fight against cyber crime".[161] The Communication does not specifically mention "cyber security", but states that the fight against cyber crime is a core element of the security of information systems. As the Commission has limited powers in the field of criminal law, the proposed approach can be only a complement to the actions undertaken by Member States and other bodies, and as put down in the Communication, the Commission is willing to support the most important actions both financially[162] and policy-wise.[163]

While the measures introduced in the III pillar instruments were mainly oriented towards securing the information society infrastructure from the common market perspective, the newest developments in the EU indicate a wider approach to cyber security. At a recent meeting of an industry body, the Messaging Anti-Abuse Working Group, in Holland, Radomir Jansky, a senior

---

[159] *Ibid*, Recital 1.

[160] See press release at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463 (last accessed June 25, 2011).

[161] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions on Towards a general policy on the fight against cyber crime (COM (2007) 267) final, and the Impact Assessment Report available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/T-CY%20_2007_%2002%20-%20e%20-%20Cybercrime%20and%20the%20EU_en.pdf (last accessed May 5, 2011).

[162] Enacted by Council Decision 2007/125/JHA of 12 February 2007 establishing for the period 2007-2013, as part of the General Programme on Security and Safeguarding Liberties, the Specific Programme "Prevention of and Fight against Crime", more information available at http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm (last accessed May 5, 2011).

[163] Eneken Tikk, Anna-Maria Talihärm. Cyber Security in European Union Legal and Policy Documents, p. 18. – CCD COE Publishing, 2008.

cyber crime official in the Commission, said new legislation was vital. "We need new legislation to fight cyber attacks. Large-scale attacks are on the rise but penalties…are not severe enough to dissuade criminals /…/ The cost for businesses, law enforcement and state authorities is on the rise, and we need to recognise that." The Commission also wants to create an EU-wide reporting system so nations can raise the alarm over attacks, and data on attacks can be collected and aggregated.[164]

This indicates that from a business and market-oriented approach the EU has widened its cyber security agenda to address also large-scale and politically motivated cyber attacks and focus on collective measures against cyber attacks.[165]

In 2009, the Computer Network Operations Concept of the European Union was adopted. As noted by Wing Commander Chris Stace, one of the authors of the concept, this is just one step towards a comprehensive coverage of cyber security in the EU.[166]

1.6.3. Council of Europe

The Council of Europe (CoE) has looked at cyber security primarily from the cyber crime angle. In 2001 the CoE introduced the Cybercrime Convention – the instrument intended to support a common criminal policy aimed at the protection of society against cybercrime.[167] The US Department of Justice has been referred to as an instrumental player in the development of the final

[164] Tom Young. EU wants new cyber crime legislation. 15 June 2009. Available at http://www.computing.co.uk/computing/news/2244107/eu-wants-cybercrime-legislation.

[165] Marc D Goodman, Susan W Brenner. The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology, Vol. 10, No. 2, 2002, pp. 139-223.

[166] Chris Stace, European Union Military Staff, Council of the European Union – Developments in the EU in the field of CNO. Presentation at the Cyber Conflict Conference, June 17, 2010.

[167] The Council of Europe Convention on Cybercrime (ETS 185, signed on 23 November 2001, entry into force on 1 July 2004), aiming to facilitate international cooperation, detection, investigation and prosecution of cyber crime and calls for establishing a common basis for substantive and procedural law and for jurisdiction, is open for signature by the member states and the non-member states which have participated in its elaboration and for accession by other non-member states. As of December 2010 the total number of signatures not followed by ratifications is 17; the total number of ratifications/accessions is 30 (Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, The former Yugoslav Republic of Macedonia, Ukraine and as a non-member the United States). Available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

accord.[168] According to Froomkin, it is widely believed that the US wrote this and pushed it through the Council, both to get access to foreign communications and especially to impress on Congress that Carnivore *[an email and electronic communications monitoring software employed by the FBI]* in the US should be seen as business as usual, and something demanded by its allies.[169]

These assertions are to an extent supported in Kristin Archick's CRS Report for Congress:

> Both the Clinton and Bush Administrations worked closely with the Council of Europe on the Convention. US policymakers assert that the Convention will not require implementing legislation; the United States will comply with the Convention based on existing US federal law. Proponents assert that many of the Convention provisions reflect the spirit of several Congressional measures that relate to cybercrime, cyber terrorism and cyber security, including the USA PATRIOT Act[170] and the Homeland Security Act[171].[172]

The Cyber Crime Convention is often referred to as the key solution to cyber security issues. Articles 2–13 of it address substantive criminal law requiring the states to criminalise cybercrime. The Convention lists offenses against the confidentiality, integrity, and availability of computers, data, and systems, computer forgery and fraud and content-related offenses as well as intellectual property and privacy infringement. Articles 14–22 address procedural law, including electronic evidence, appropriate powers and procedures for investigations. It covers, inter alia, system search and seizure, real-time collection of traffic data, interception of content data, and the preservation and rapid

[168] Sylvia Mercado Kierkegaard. Cracking Down On Cybercrime Global Response: The Cybercrime Convention. – Communications of the IIMA. 2005, Volume 5 Issue 1. Available at http://www.iima.org/CIIMA/CII-MA%205.1%2059%20Kirkegaard-7.pdf (last accessed May 5, 2011).

[169] Michael Froomkin. Cybercrime Treaty Goes Live. Discourse.net, 19 March 2004. Available at http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html (last accessed May 5, 2011).

[170] (Public Law 107-56, introduced as H.R. 3162 by Rep. James Sensenbrenner in October 2001) authorises the interception of electronic communications for the collection of evidence related to terrorism, computer fraud, and abuse (Sections 201 and 202) and clarifies the definition of protected computers and increases fines and prison terms for damage (Section 814).

[171] (Public Law 107-296 introduced as H.R. 5005 by Rep. Richard Armey in June 2002) directs the US Sentencing Commission to re-evaluate federal sentencing guidelines for crimes involving computer-related fraud and hacking offenses, especially against restricted federal government systems (Section 225, the Cyber Security Enhancement Act of 2002).

[172] Kristin Archick. Cybercrime: The Council of Europe Convention. CRS Report for Congress, 22 July 2004. Avaiable at: http://fpc.state.gov/documents/organisation/36076.pdf (last accessed May 5, 2011).

disclosure of computer-stored data relating to traffic. Articles 23–35 are devoted to international cooperation.[173]

However, as Künnapu's analysis indicates, the implementation of the Convention is not uniform and often does not correspond to emerging national security-relevant threats.[174]

As Künnapu reports,

> "During the T-CY meeting in 2008 practical aspects concerning the implementation of the Convention were discussed. It was noted that question of jurisdiction should be considered in light of technological developments and problems concerning the location of the server and how law enforcement authorities should respond if the location is rapidly changing (dynamic DNS, fast-flux DNS)."[175]

Problematically for national cyber security interests, under Article 27 (4) a) and b) of the Convention, cooperation and assistance may be refused if the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence or in case execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. These restrictions pose a substantial restriction to the applicability of the Convention to politically motivated cyber attacks and suggest that the Convention was not meant to deal with politically or ideologically motivated cyber attacks in the first place.

The growing sophistication and breadth of criminal activity highlight the potential for malicious activity in cyberspace to affect national competitiveness, cause a general erosion of trust in the use of the Internet for commerce and trade, and cripple civil infrastructure. The volume and scope of these activities are increasing. According to a recent CoE report, the increased dependency on ICT results in growing vulnerability to criminal misuse and attacks. The CoE notes the rapid expansion of online fraud and the trends of cybercrime increasingly aiming at generating illegal proceeds and offenders organizing to commit crime on the Internet. In response to this trend, the CoE urges governments towards effective criminalisation of cyber offenses; investigative and prosecutorial procedures and institutional capacities allowing criminal justice agencies to cope with cyber crime; facilitating direct cooperation

---

[173] See also, Mike Keyser. The Council of Europe Convention on Cybercrime. – Journal of Transnational Law & Policy, Vol 12:2, Spring 2003, pp. 287-326; Shannon L. Hopkins. Cybercrime Convention: A Positive Beginning to a Long Road Ahead. – Journal of High Technology Law, Vol II No. 1, 2003, pp. 101-122.

[174] Markko Künnapu. Council of Europe Convention on Cybercrime. European Union Framework Decision on attacks against information systems: Comparative study on the implementation and recent developments. – A research paper for the Cooperative Cyber Defense Centre of Excellence, 2008. Unpublished.

[175] Opinion of the Committee of Experts on Terrorism (CODEXTER) on cyberterrorism and use of Internet for terrorist purposes. – Strasbourg: The Cybercrime Convention Committee (T-CY), 12 March 2008, document T-CY (2008) INF 02 E.

between State institutions as well as between public and private sector and efficient mutual legal assistance regimes.[176] Expected additions to Cyber Crime Convention include topics like cloud, jurisdiction and higher sanctions.

Further critique to the Convention includes the observations of Judge Schjølberg about the Convention being based on the criminal conducts of late 1990s and not covering techniques such as phishing, botnets, spam, cyber terrorism; and the terminology of the Convention being 1990s terminology, and not necessarily suitable for the 2010s.[177]

1.6.4. OSCE

The world's largest security organisation has been active in cyber security mainly from the perspective of cyber terrorism. The Action against Terrorism Unit has since 2002 coordinated and facilitated OSCE programmes relevant to the struggle against terrorism. In 2010, in an OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security, the delegates agreed that the role of OSCE in the global cyber security needs to be redefined: "Concerned with the sophistication of online malicious activities, the OSCE has decided to intensify the action by enhancing international co-operation on countering the use of the Internet for terrorist purposes; to consider taking all appropriate measures to protect vital critical information infrastructures and networks against the threat of cyber attacks; to consider becoming party to and to implement their obligations under the existing international and regional legal instruments; and to explore the possibility of more active engagement of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes."[178]

Since 2009 OSCE has promoted a more comprehensive approach to cyber security. Such an approach is based on the understanding that the widespread use of the Internet by terrorists, traffickers and criminals make it increasingly difficult to develop effective responses to transnational threats without promoting a more secure cyberspace. A comprehensive approach to cyber security should: (a) strengthen national security; (b) tackle cybercrime; (c) inhibit terrorist use of the Internet; (d) be responsive to a wide variety of risks and threats, including politico-military dangers; (e) enable competent authorities to protect a wide spectrum of targets ranging from the individual Internet user to critical infrastructures; and (f) safeguard the Internet as a space for free expression and assembly.[179]

---

[176] Council of Europe Project on Cybercrime Final Report. – Strasbourg: Economic Crime Division of the Directorate General of Human Rights and Legal Affairs, 14 May 2009. Document ECD/567(2009)1.
[177] *Supra nota* 16, p. ii.
[178] OECD MC.DEC/7/06.
[179] Report by the OSCE Secretary General on the Implementation of MC.DEC/2/09 on Further OSCE Efforts to Address Transnational Threats and Challenges to Security and

How OSCE will furnish its comprehensive mandate is yet to be defined. The US defines potential OSCE activities within the comprehensive approach as follows:

> National action plans or strategies – The OSCE could promote the development of national action plans or strategies – perhaps based initially on the proposed survey and self-assessment – that would outline essential national priorities in securing cyberspace.
> Legislation – The OSCE could support efforts to develop harmonised national and international frameworks for responding to cybercrimes, including by gaining private sector cooperation for investigation and prosecution.
> Law enforcement cooperation – The OSCE could help establish the practice and expectation of effective cooperation between participating States' law enforcement agencies on cyber security issues. Sometimes this could mean the adaptation of uniform cooperative arrangements to the unique nature and speed of cyber security incidents.
> CERT information sharing – The OSCE could consider the extent and degree to which participating States have established national Computer Emergency Response Teams (CERTs) by identifying core elements of the CERT capability that should be common to all participating States.
> Public-Private Partnerships – The OSCE could develop ongoing and incident-specific frameworks for partnerships between government and the private sector, with added focus on working with global ICT firms that have significant influence over the development of cyberspace.
> Education and awareness – The OSCE could establish the best practices in education and awareness raising among a wide range of societal sectors to help promote a culture of cyber security awareness among all users.
> Strengthening the OSCE's mandate – Building on existing OSCE mandates of relevance to cyber security, a new mandate could be sought that specifically tasks the organisation to further engage in comprehensively enhancing cyber security.[180]

On OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role the action items for the organisation were defined to focusing on the politico-military dimension of cyber security, consolidating national views on norms of behaviour within a politico-military context building on existing international law, ensuring shared values of human rights and fundamental freedoms while countering threats emanating from cyberspace, discussing pertinent terminology as agreement on terms/definitions is crucial and elaborating a potential strategic framework in the area of comprehensively enhancing cyber security.[181]

Stability. Available at http://www.delegfrance-osce.org/IMG/pdf/sec_gal_107_sg_report_on_TNT.pdf (last accessed May 5, 2011).

[180] US Delegation to OSCE proposal „An OSCE Strategy for a Comprehensive Approach to Cybersecurity" March 1, 2011.

[181] OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role, 9-10 May 2011 Vienna, Draft Report on the Proceedings.

1.6.5. UN

With 194 members, the UN is quantitatively the most powerful player among international organisations. ITU is an intergovernmental organisation within the UN system that has partnerships between government and industry. While ITU has recently engaged in the fight against cyber crime, the activities of the UN itself have been targeting cyber arms control and the overall process of making information technology and telecommunications more secure. The most recent manifestation of UN interest in the field is the report of the Governmental Expert Group. Among other observations the Expert Group noted: "Non-criminal areas of transnational concern should receive appropriate attention. These include the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to State use of ICTs, which could affect crisis management in the event of major incidents. This argues for the elaboration of measures designed to enhance cooperation where possible. Such measures could also be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability."[182]

The Expert Group has also expressed its view on the need for additional regulation, noting that existing agreements include norms relevant to the use of ICTs by States.[183] Realizing that among a forum of 194 countries the priorities and capabilities for enhancing global cyber security differ, the Group also asserted:

> Capacity-building is of vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security.[184]

UN as an international organization has unique features. Its membership comprises 194 countries and its activities range through virtually all aspects of information society and its security. At the same time the strengths of the UN can also work as weaknesses when it comes to coordinating nuance-rich cyber security.

1.7. Changed Scope of Protection

When US National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Richard Clarke was asked on a press briefing in 2000: "What's the biggest threat that we need to guard against? Is it hackers and vandalism? Is it criminals? Or is it domestic or foreign terrorism?", he responded: "I think it's all of the above. There's a spectrum, from the teenage hacker who

[182] *Supra nota* 131, para 14.
[183] *Ibid*, para 16.
[184] *Ibid*, para 17.

sort of joy rides through cyberspace, up through industrial espionage, up through fraud and theft. And up at the far end of the spectrum, to another country using information warfare against our infrastructure."[185]

The "lower end" threat of this spectrum – cyber crime – has received wide attention in the past decade. The development and current state of cyber crime is discussed in more detail in section 3.8 of this dissertation. As Vogel explains, there is no universally accepted definition of cybercrime as such. /…/ Accordingly, the scope of specific cyber offences is not limited to manipulating or sabotaging computers. Rather, modern cyber offences relate to a variety of harmful behaviours linked with information systems and/or data […].[186] This means that the notion of cyber crime changes by jurisdiction thus making it difficult to expect cooperation from national authorities.

The first wave of the highest level of threat on the spectrum of cyber conflict – cyber warfare[187] – is primarily associated with the United States and dates back to early 80-ies. Publicly known cases include the transfer by the United States of software for Soviet pipeline pumps with embedded features to cause pump speeds and valve settings to malfunction and resulting in the „most monumental non-nuclear explosion and fire ever seen from space".[188] Although the United States report cyber warfare capabilities from other countries, this information is not backed up by extensive references and is more an estimate than fact. Backed-up data is available about cyber warfare capabilities in China.[189]

When the attacks against Estonia happened in 2007, the concern for cyber warfare was introduced more widely on international level and the attention of the European countries was drawn to the network-centric lifestyle and dependence on ICT as a national security concern.

Categorizing cyber incidents will always be challenging due to the variety of opinions involved. Veerasamy and Taute conclude that much misconception exists over whether an attack on the network is information warfare, cybercrime,

---

[185] White House Press Briefing by Chief of Staff John Podesta, Secretary of Commerce Bill Daley, James Madison University President Linwood Rose and National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Dick Clarke on January 7, 2000. Available at http://cryptome.org/cybersec-wh.htm (last accessed May 5, 2011).

[186] Joachim Vogel. Towards a Global Convention against Cybercrime. First World Conference on Penal Law. Penal Law in the 21st Century. 2007, p. 1-2.

[187] Cyber warfare is the use of computer intrusion techniques and other capabilities against an adversary's information-based infrastructure to intentionally affect national security or to further operations against national security. *Supra nota* 24. Information warfare comprises information operations (actions taken to affect adversary information and information systems while defending one's own information and information systems) conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. US Dep't of Def., Joint Publication I-02 ,Dictionary of Military and Associated Terms 129 (1998).

[188] *Supra nota* 6, page 2–3,

[189] Ibid, page 3-4.

or cyberterror.[190] Major Adkins[191] offers a cyber security spectrum covering cyber crime[192], hacktivism[193], cyber espionage[194], cyber terrorism[195] and cyber warfare[196]. A CRN Report from 2009 takes a comprehensive approach to actors, referring to recently adopted and/or revised national cyber security policies.[197] It distinguishes 'established capable states', 'terrorist organisations, organised criminals and state-sponsored actors', and 'online criminals' as malevolent actors threatening cyber security.[198] It offers a developed version of Denning's categorisation of cyber security threats[199] by presenting a ladder of threat rungs covering activism[200], hacktivism[201], cybercrime[202], cyberterrorism[203] and

[190] N. Veerasamy, B. Taute. An Introduction to Emerging Threats and Vulnerabilities to Create User Awareness. – Council for Scientific and Industrial Research. 2009.

[191] Bonnie N. Adkins. The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role? – A research report submitted to the faculty in partial fulfilment of the graduation requirements. Alabama, 2001. Available at http://www.stormingmedia.us/94/9496/A949604.html (last accessed May 5, 2011).

[192] *Ibid*, p. 34. Cyber attacks without the intent to affect national security or to further operations against national security.

[193] *Ibid*, p. 9. Hacktivism /…/ represents a political motivation with intent to not only do harm to a system, but to influence the public and government that it is protesting with its electronic civil disobedience.

[194] *Ibid*, p. 26. Cyber-espionage is the use of computer hacking in foreign intelligence operations to obtain information or access to foreign computer systems with the intent to commit espionage or have the access to commit state sponsored sabotage when necessary.

[195] *Ibid*, p. 26. Adkins uses Denning's definition of Cyber Terrorism: Cyber-terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data, which result in violence against noncombatant targets by subnational groups or clandestine agents.

[196]Ibid, p. 27. The use of computer intrusion techniques and other capabilities against an adversary's information-based infrastructure to intentionally affect national security or to further operations against national security..

[197] Focal Report 3: Critical Infrastructure Protection. Cybersecurity – Recent Strategies and Policies: An Analysis. Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich. Zurich, 2009. Available at http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=108743 (last accessed May 5, 2011).

[198] *Ibid*, p. 7.

[199] *Supra nota* 26.

[200] S*upra nota* 197, p. 16. Normal, non-disruptive use of the internet in support of a (political) agenda or cause.

[201] *Ibid.*, p. 16. "Marriage" of hacking and activism, including operations that use hacking techniques against a target's internet site with the intention of disrupting normal operations.

[202] *Ibid.*, pp. 16-17. Includes theft of intellectual property, extortion based on the threat of Distributed Denial of Service attacks (DDoS) attacks, fraud based on identity theft, etc. The intention of the attacker is economically driven.

[203] *Ibid*., p. 17. Consists of unlawful attacks against computers, networks, and the information stored therein, to intimidate or coerce a government or its people in furtherance of political or social objectives. Such an attack should result in violence against persons or property, or at least cause enough harm to generate the requisite fear level to be considered cyber-terrorism.

cyberwar[204]. The CRN Report thereby responds to the concern reflected in the Estonian cyber strategy about the absence of common definitions of [cyber] threats[205] and lines up part of the cyber threat spectrum by indicating actors relevant to criminal law and the Law of Armed Conflict.

Dr. Lachow distinguishes between motivation, methods and targets of cyber terror, hacktivism, cracking, cyber crime, cyber espionage and state-level info war.[206]

	MOTIVATION	TARGET	METHOD
Cyber Terror	Political change	Innocent victims	Computer-based violence or destruction
Hactivism	Political change	Decision-makers	Attack
Cracking	Ego, personal enmity	Individuals, companies, gov'ts	Attach, Exploit (sometimes overt)
Cyber Crime	Economic gain	Individuals, companies	Fraud, ID theft, blackmail, Attack, Exploit
Cyber Espionage	Economic gain	Individuals, companies, gov'ts	Attack, Exploit (rarely overt)
State-Level Info War	Political or military gain	Infrastructure, military assets	Attack, Exploit, physical attack

Lachow's Chart.

Recent threat assessments indicate that cyber security threat perception covers different actors, motivation and targets. As concluded by the Crisis and Risk Network (CRN) Center for Security Studies (CSS), cyber threats affect either economic well-being or national security and are posed by state and non-state actors. CRN CSS lists cybercrime, cyber terrorism, cyberwarfare and industrial spying among those affecting critical information infrastructure.[207]

Dr. Paul Cornish from the Chatham House lists the cyber threats on four levels: hacking, serious and organized crime, ideological and political extremism and state-sponsored cyber aggression.[208]

---

[204] *Ibid*., p. 17. Use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems.
[205] *Supra nota* 197.
[206] Irving Lachow. Cyber Security: A Few Observations. – National Defense University. 2008.
[207] *Supra nota* 197, page 9.
[208] Supra nota 116, page 7-16.

Another widely acknowledged categorization of threats and responses to them was the computer network operations (CNO) model comprising computer network attack[209] (CNA), computer network defense[210] (CND) and computer network exploitation[211] (CNE). However, as Chabinsky concludes, this model broke down because the definitions lack clear legal and policy distinction and often bleed between themselves.[212]

Various threats are defined by actors and their methods rather than by specific action or target. As Denning writes, current cyber conflict is emerging at the expense of social networks of non-state actors who launch cyber attacks for social andpolitical reasons. She explains that malicious actors exploit popular social networks to articulate their goals, plan and announce attacks, encourage people to participate, disseminate tools and instructions as well as acquire information about their targets and potential supporters. The attackers also manage their own online forums and develop and acquire software tools to be used to attack.[213] According to Denning, electronic reflections exist for jihad (i.e. cyber attacks conducted on behalf of al-Qa'ida and the global jihadist movement associated with it).

Hacktivism is understood as the convergence of hacking with activism that mostly manifests either in defacement of websites with political and social messages (e.g. Estonian Reform Party website in April 2007, Georgian President's website in August 2008 etc.) or denial-of-service (DoS) attacks that disrupt access to target websites, usually by flooding them with traffic.[214]

Denning separates patriotic and nationalistic hacking from hacktivism, referring to it as citizens and expatriates engaging in cyber attacks to defend their mother country or country of ethnic origin. She explains that patriotic attacks are mainly launched against websites and e-mail accounts of countries whose actions have threatened and harmed the interests of their mother country. [215] After 2007 attacks, Estonia introduced the concept of cyber

[209] Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. – Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02, 12 April 2001, Amended Through 30 September 2010, p. 93. Available at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (last accessed May 5, 2011).

[210] *Ibid*. Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.

[211] *Ibid*. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

[212] Steven R. Chabinsky. Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line. Journal of National Security Law & Policy, Volume 4 (27), 2010, page 31.

[213] Dorothy E. Denning. Cyber Conflict as an Emergent Social Phenomenon. – Thomas J. Holt (Ed.), Bernadette H. Schell (Ed.) Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications, 2011.

[214] *Ibid*.

[215] *Ibid*.

terrorism in the Penal Code[216] and later also revised national emergency regulation from cyber perspective[217], thereby regarding cyber security as national security issue and introducing relevant defense and response mechanisms. Denning further observes that in the presence of both motivated actors and vulnerabe systems, cyber terrorism could morph from the largely theoretical threat it is today to something real.[218] At the same time, Lewis defines cyber terrorism as the use of computer network tools to shut down critical national infrastructure or to coerce or intimidate a government or civilian population, thus categorizing the Estonian incident as such.[219]

Denning warns, however, that fair assessment is needed as to under which circumstances to label a denial-of-service attack cyber warfare, referring to the need to examine the details of specific operations as regards to duration, impact on national functions, loss of life and destruction of and damage to property.[220] The law of armed conflict and humanitarian law bring about military involvement and thus need to be carefully assessed as response mechanism to cyber attacks.

Each of these categories and rungs can be affiliated with one or more legal terms potentially applicable to a specific activity. While activism would be covered by regular IT security legal framework-setting limitations to spreading of spam and using personal data, most forms of hacktivism, cyber crime and cyber terrorism would fall in the area of criminal law and cyber crime regulation. National security relevant cyber incidents would require additional attention from national security law perspective and cyber warfare would be a term relevant for IHL/LOAC application.

So far, responses to cyber incidents have been developed primarily from the single victim and individualised threat perspective, whereby every entity and individual would assess and mitigate threats resulting from his/her conduct or business model. Also, as explained by Wulf and Jones, so far most research on cyber security has been based on the assumption that the "thing" we need to protect is "inside" the system. Therefore, we have developed "firewalls" and other mechanisms to keep "outside" attackers from penetrating our defences and

---

[216] In 2008 Estonian Penal Code § 237 „Acts of terrorism“ was amended to include “interference with computer data or hindrance of operation of computer systems as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population counted among acts of terrorism.”. Penal Code (consolidated text Apr 2008) available at
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistus

[217] The Emergency Act, RT I 2009, 39, 262.

[218] *Supra nota* 213.

[219] See James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. CSIS, Washington, DC, December 2002.

[220] *Supra nota* 99.

gaining access to the thing and taking control of the system. This perimeter defence model of computer security – sometimes called the Maginot Line model – has been used since the first mainframe operating systems were built in the 1960s. Unfortunately, it is dangerously, even fatally, flawed.[221]

With politically motivated cyber attacks, individual threats are extended and accompanied by the risk of occurring among a collective of victims and thus being exposed to (and potentially involved in) threats and attacks not directly related to one's own behaviour or position. This makes it vital for effective defence to understand the perspectives beyond one's own – be it legal, technical or political. Without realizing the surrounding cyber security situation the defences we build remain inefficient.

Cyber threats cannot be regarded in isolation from the general peace and security picture. As cyber threats become more asymmetric, defences require extensive coordination both on national and international levels. An example of acknowledging and coordinating cyber responses as part of the overall defence investments, processes and capabilities is NATO's concept of hybrid threats, picturing cyber as one component of a possible asymmetric attack. No nation or corporation these days is truly in a position to face and manage cyber threats on its own – the global architecture of networks, along with different stakeholders involved in administering the systems, makes it impossible to enforce security only within organisationally or territorially defined jurisdictions. This conclusion also served as a basis of drafting the 2001 Council of Europe Convention on Cybercrime.[222]

On the national level, coordination of efforts between different authorities and expertise is required.[223] On the international level, the vectors of coordination involve international organisations offering assistance and advice in case of a cyber attack, countries and entities in possession of expertise and information necessary for mitigating the attacks as well as countries whose infrastructure is used to launch the attacks.

[221] William A. Wulf, Anita K. Jones. Cybersecurity. – National Academy of Engineering Publications, Vol. 32, No. 1, March 2002.

[222] For more information on this, see the Explanatory Report to the Council of Europe Cybercrime Convention (ETS 185). Available at http://conventions.coe.int/treaty/en/reports/html/185.htm (last accessed May 5, 2011).

[223] Controlling crime involving digital technology and computer networks will require a variety of new networks: networks between police and other agencies within government, networks between police and private institutions, and networks of police across national borders. See Roderic Broadhurst. Developments in the Global Law Enforcement of Cyber Crime. – International Journal of Police Strategies and Management. Vol. 29, Issue. 3, p. 411.

1.8. Calls for a Comprehensive Approach

As earlier approaches to cyber security become obsolete, proposals emerge for an approach that would make use of the measures implemented so far and enhance them so as to adequately respond to the new threat picture.

OSCE has noted that cyber security can only be achieved via an approach that strengthens national security, tackles cyber crime, inhibits terrorist use of internet, is responsive to a wide variety of risks and threats, including the political and military ones, enables competent authorities protecting a wide spectrum of targets ranging from critical infrastructure to individual users, and at the same time safeguards free speech and privacy.[224] Any fragmented approach is doomed to failure, OSCE's Cyber Terrorism expert Nemanja Malisevic concluded in his presentation at the Cyber Conflict Conference in Tallinn.[225] Calls for a comprehensive approach to cyber security also come from NATO[226], the EU[227] and other influential international organisations.

A comprehensive defence in the cyber context requires getting rid of a stove-piped approach to cyber security planning and encourages synergy between information society design, criminal policy planning, law enforcement capabilities and military defence. This approach has been introduced earlier in the cyber crime context – in 2004, OECD noted that combating Internet fraud requires a higher degree of international cooperation than the one that exists presently, with an integrated crime prevention strategy that will address primary prevention, target hardening and deterrence. Such a strategy would, according to OECD, incorporate an effective anti-spam law in all countries; cross-border cooperation of enforcement in specific cases; self-regulatory solutions by market players, for example on contractual and marketing practices; technical solutions to manage or reduce spam, like filtering and other security features; greater consumer awareness /.../.[228]

As Broadhurst observed in 2006, over the past decade, considerable progress has been made within and between nations to develop the capacity of police to respond to cybercrime and there is now growing awareness amongst computer users of the need for basic security on-line. Yet the pace of technological

---

[224] *Supra nota* 180.

[225] Nemanja Malicevic. Recent Initiatives and Plans at the OSCE. – Presentation at CCD COE Conference on Cyber Conflict, Tallinn, 17 June 2010.

[226] A Comprehensive Approach. Available at http://www.nato.int/cps/en/natolive/topics_51633.htm (last accessed May 5, 2011).

[227] See, e.g., EU-US Summit Joint Statement. Lisbon, 20 November 2010. Available at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/117897.pdf (last accessed May 5, 2011).

[228] OECD Work on Spam, 2004. Available at http://www.oecd.org/sti/spam/ (last accessed May 5, 2011). EU statement on OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role (Opening Session) (PC.DEL/420/11, 9 May 2011) page 2: [T]he efforts at international level should be primarily focused on the actual implementation of existing tools and instruments, while providing for consolidated approach in capacity building and technical assistance in developing countries.

change will continue unabated, and the adaptability of cyber-criminals will continue to pose challenges for law enforcement. [229]

As concluded in an article aimed at defining NATO's role in global cyber security among other international institutions and in national efforts –

> "The call for a comprehensive approach to cyber security is driven by the necessity to move beyond a largely inefficient sectorial approach in cyber security development and cyber incident management. This need has been recognised both on organisational and national level. However, there is still no universal single definition for the term.
> There are many factors directing the definition/concept of comprehensive approach. For one, a comprehensive approach is necessary because of the multifaceted nature of the threat landscape: cyber threats vary from mass cyber attacks fuelled by a political agenda to highly precise and sophisticated attacks targeting vital national interests; at the same time, cyber threats are also fast-evolving. This makes it impossible to give a once-and-for-all catalogue of cyber threats – a more inclusive approach is necessary.
> Secondly, the environments in which these threats manifest differ. Countries are not similar in terms of their ICT penetration and reliance on communication and information technologies; they have differing interests and priorities. Yet due to the borderless nature of cyber threats, cross-border cooperation is unavoidable, and this requires a certain level of harmonisation of perceptions and of activities. Any incident management regime, including the legal one, must facilitate and support coordination and cooperation.

Also importantly, building up a secure cyber environment and cyber incident management is a cooperative effort of several different fields of expertise. Technological issues are to be solved by technological, not legal measures – but law must be able to support the technological capabilities." [230]

Country-wise, the United States was the first to propose a comprehensive cyber security agenda. [231] In early 2009 the White House published its Comprehensive National Cybersecurity Initiative identifying cyber security as one of the most serious economic and national security challenges the nation faces and ordering a thorough review of federal efforts to defend the US information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.[232]

When proposing a comprehensive approach to information security for the OSCE, the US explained the benefits of this approach as follows:

---

[229] *Supra nota* 223, pp. 418.
[230] S*upra nota* 133.
[231] James A. Lewis et al. Securing Cyberspace for the 44th Presidency. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. – Washington: 2008. Available at http://csis.org/files/media/csis/pubs/08-1208_securingcyberspace_44.pdf (last accessed May 5, 2011).
[232] http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last accessed May 5, 2011).

> "While seeking ways to tackle the use of cyberspace for criminal and terrorist activities, the OSCE is also well-placed to ensure that the freedom of expression and association are adequately protected. With its broad membership and wide array of existing political commitments, the OSCE can provide a managed peer review process that could prod individual participating states into action in a way that a broader international approach, with fewer mechanisms to promote accountability, might not."[233]

A comprehensive approach has also been discussed and promoted by other international organisations. The UN expert group has outlined the need for a comprehensive approach from the perspective of the threat spectrum.

> "The [cyber] threat spectrum emanates from a wide variety of sources including natural disasters and a diverse range of man-made events. While some are State-based, many come from non-State actors and involve criminal activity. Disruptive activities in cyberspace target individuals, corporations, critical national infrastructures, and governments alike. Their effects carry significant consequences for the security of nations and the globally-linked international community as a whole.[234] The use of proxies to conduct disruptive operations using information technology presents new challenges for States. The use of ICTs for disruption significantly increases States' ability to engage in attacks with plausible deniability."[235]

Similarly, the EU has expressed its concern about the threat spectrum that cannot be mitigated by stove-piped strategies, means and methods:

> "Different types of cyber attacks have taken place in recent years; reaching from the planting of malicious software on personal computers and defacing of public websites to the penetration of databases and secure communication networks and well-coordinated, massive attacks against national critical infrastructure and public institutions of the EU Member States. Individuals, organised crime and terrorist entities may all be involved, but there is also growing evidence that politically motivated attacks are being carried out by state-inspired or state-sponsored entities but also by government agencies. Cyber attacks may also be launched prior to or in support of military operations."[236]

With reference to Internet governance discussions in the framework of the World Summit on the Information Society in 2003–2005, Andjelkovic conclu-

---

[233] An OSCE Strategy for a Comprehensive Approach to Cybersecurity (Draft as of March 1, 2010), p. 2.
[234] *Supra nota* 131.
[235] *Ibid*.
[236] Cyber Security: What Role for CFSP? – EU Institute for Security Studies Report. 10 March 2009, p. 2. IESUE/SEM(09)04 Available at http://www.iss.europa.eu/fileadmin/fichiers/pdf/seminars/2009/Report_cyber_-security.pdf (last accessed May 5, 2011).

des that Internet governance cannot be purely a matter of legal regulation, but a combination of legal and non-legal approaches.[237]

National approaches to cyber security also tend to see it as a spectrum of threats and approaches. As Dylevskii and Komov suggest, the program of legislation in the sphere of the public law of the Russian Federation must focus on the promotion of the politico-legal concept of the public policy covering, on the whole, the military, criminal and terrorist aspects of ensuring trans-border information security.[238]

To sum up, it follows from national and international observations that none of the narrow or specialised perspectives to cyber security can be exhaustive. A comprehensive approach to cyber security combines the elements of threat, deterrence and response from different areas of authority and responsibility, thereby eliminating gaps between relevant areas and highlighting overlaps of authority. From a defence perspective, a comprehensive approach reduces the likelihood of a cyber attack resulting in an *ad hoc* reaction or falling into a legal or policy loophole.

An approach like this optimises the roles and responsibilities of different authorities and stake-holders in securing the cyber domain and managing a cyber incident. In addition, it focuses on the substantive measures available for cyber security, using the frameworks of cyber security and individual responsibility as a background system for implementing defences against individual threat factors such as botnets, spam, malware, etc. This allows for more creativity in tackling individual information security areas such as data and privacy, e-commerce, or terrorist use of Internet.

Comprehensive defence in the cyber context requires getting rid of a stove-piped approach to cyber security planning, and encouraging synergy between information society design, criminal policy planning, law enforcement capabilities and military defence. The contemporary nature of cyber threats requires practical reinforcement of different lines of action along with additional instruments to cover the whole spectrum of cyber threats, including those of national security relevance.

The following chapter will look at the elements of a comprehensive approach, and identify stakeholders, perspectives and elements of cyber security to be considered when developing national responses to contemporary cyber conflicts.

---

[237] Maja Andjelkovic. Internet Governance: In the Footsteps of Global Administrative Law. – University of Kent Law School. September, 2006.

[238] I. N. Dylevskii, S. A. Komov et al. Russian Federation Military Policy for Provision of International InformationS ecurity. – Military Thought, 2006, Volume 15, Issue 2.

CHAPTER II.
STRUCTURAL FRAMEWORK FOR INTERNATIONAL CYBER SECURITY

A comprehensive approach to cyber security requires a combination and coordination of tools, methods and approaches to enhance the global cyber security environment. An ideal combination would serve and balance the purposes and concerns of technology, policy and law. In other words, cyber security will need to be based on technological developments and the underlying architecture of the information society, correspond to current national and international policy concerns and ultimately, materialise in a regulatory framework supporting the former two.

There are a number of challenges related to taking an approach like this from the legal perspective. First, there are different fields of legal expertise involved in cyber incident management, requiring skills in information society/telecommunications law, criminal law, national security law and law of armed conflict. Wide-ranging expertise like this is currently rare among legal professionals.

Second, providing appropriate legal responses requires an understanding of the underlying situation, terminology and concepts of information and communications technology, and therefore presumes an understanding of the basics of information technology or coordination between the legal and technology communities. This may be difficult, since the legal areas dealing with cyber security need to constantly adapt to developments in technology and the information society. Moreover, often the concepts of the legal areas involved have not been agreed upon by a wider international community, and in some legal areas the cyber aspect has been less integrated than in others.

Third, a concerted approach to cyber security is challenged by the fact that policy responses and leads, which ultimately have to support the process of legislation and incident handling, have been based on different concepts, terminology and priorities. A good example of the law-policy-technology dichotomy is the notion of cyber security itself, examined in more detail in Chapter I of this dissertation.

Furthermore, in most cases the details of national cyber security legal and policy decisions and solutions are not transferable to other nations – simply because the state administration, legal system or information society characteristics differ extensively by jurisdiction. Therefore, although for Estonia and Georgia cyber threats have materialised enough to develop new and nationally comprehensive responses[239], the context of and approaches to these threats cannot be transferred to other jurisdictions and entities without critical

[239] See Kadri Kaska, Anna-Maria Talihärm, Eneken Tikk. Developments in the Legislative, Policy and Organisational Landscapes in Estonia Since 2007. – International Cyber Security Legal & Policy Proceedings. CCD COE Publishing, 2010, pp.40-66.

thinking.[240] At the same time, cases and best practices have proved that there are elements in global cyber security that need attention regardless of individual threat factors such as the architecture of a specific network or the bandwidth available for a specific service.

Because of different disciplines and perspectives involved in cyber security planning and management, it is often challenging to narrow down the discussion to the point where conclusions and arguments would be understood and supported in the same way by all experts and scholars involved. For example, a question about the legality of "hack back" has kept coming up in the context of cyber security discussions for more than a decade now[241], but has never been answered exhaustively.[242] "Hacking" is defined as a term to describe an unauthorised user who attempts to or gains access to an IS[243], but is also popularly used as a negative connotation for "someone who breaks into computer systems without authorisation"[244]. The means and methods as well as motivation for gaining unauthorised access are so different that it is impossible to cover them all in an abstract legal analysis.

The corresponding legal constructs under the Council of Europe's Convention on Cybercrime potentially include "the access to the whole or any part of a computer system without right"[245], "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system"[246], data and system interference[247], as well as misuse of devices[248]. It is relevant to note that other international notions of cyber crime exist and that national implementation of these instruments will create a number of nuances around "hack-back" as a means of self-defence.

To bring another example, from the legal perspective, the term "self-defence" refers to two essentially different concepts – one under criminal law and the

---

[240] See also, Eneken Tikk, Monika Mikiver. Applicability of the Census Case in Estonian Personal Data Protection Law. Juridica International, 1, 2006, pp. 102 – 110.

[241] See, e.g., Deborah Radcliff. Can You Hack Back? CNN, 1 June 2000. Available at http://archives.cnn.com/2000/TECH/computing/06/01/hack.back.idg/index.html (last accessed May 5, 2011). Joshua Davis. Secret Geek A-Team Hacks Back, Defends Worldwide Web. – Wired, 24 November 2008. Available at http://www.wired.com/techbiz/people/magazine/16-12/ff_kaminsky?currentP.=all#ixzz0uqNdRK2G (last accessed May 5, 2011). Ruperto P. Majuca, Jay P. Kesan. Hacking Back: Optimal Use of Self-Defense in Cyberspace. – Illinois Public Law Research Paper No. 08-20, 18 March 2009. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932 (last accessed May 5, 2011).

[242] V. Jayawal et al. Internet hack back: counter attacks as self-defense or vigilantism? – IEEE 2002 International Symposium on Technology and Society. Social Implications of Information and Communication Technology. Proceedings.

[243] *Supra nota 119*, p. 30.

[244] *Supra nota* 242, p. 1.

[245] Council of Europe Convention on Cybercrime (ETS 185, signed on 23 November 2001, entry into force on 1 July 2004). Article 2.

[246] *Ibid*. Article 3.

[247] *Ibid*. Articles 4 and 5.

[248] *Ibid*. Article 6.

other (individual or collective self-defence) under the Law of Armed Conflict. In both legal contexts, the analysis underlying a decision regarding the legality of a particular act requires precision and correct understanding of the underlying facts to define the terms and conditions of "hack back" and ideally offer alternatives that would be acceptable and executable from the technology and policy perspective. Also, the background of the term as used in cyber-security related discussions and papers may not be visible to non-lawyers.

Defining the international scope of cyber security is an even more difficult task. Already from a national perspective, the critical components of national infrastructure need to be defined considering the threats relevant to the nation under question. Whereas Estonia as a nation may be exposed and vulnerable to large-scale DDoS attacks that may result in the inability of the government to perform its functions, a country with no e-government solutions and wider bandwidth capabilities may see DDoS attacks as irrelevant. Depending on several factors such as the ICT penetration, geographical location, size of the population, traditional national security threats, etc., countries may have different concerns that together sum up the spectrum of cyber attacks of national relevance. On the other hand, international cyber security, if regarded as the sum of national concerns, will be a concept too broad for any meaningful action. Also, the role of international cooperation would be to fill in where nations are incapable of providing solutions on their own. Thus, international cyber security is the sum of national cyber security concerns that cannot be solved on the national level.

The aim of this chapter is not to explain in detail the differences in terminology, approaches and perceptions existing between the legal, policy and technology communities. Rather, the chapter is intended to point out the existence and possible effect of such differences and offer a framework that helps understanding and considering different aspects and perspectives of computer and network security from the legal perspective.

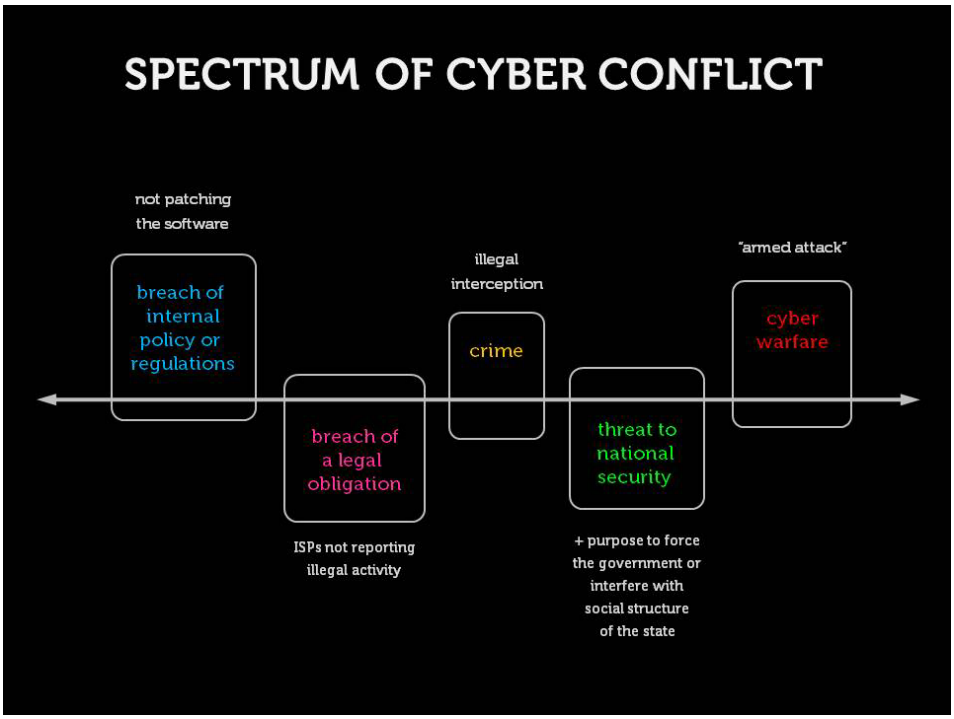
To do so, this chapter first touches upon the notion of cyber security and then proceeds to introduce a conceptual model of thinking about and developing systematic legal and legal policy responses to cyber conflict. It is intended to facilitate the comprehension of many legal nuances around decisions, regulations and law enforcement *in re* cyber incidents and to improve interaction between lawyers and other experts dealing with cyber incident management. It presents a number of prevalent views developed by scholars and practitioners involved in cyber incident handling as well as conclusions derived from the discussions with several country and organisation representatives[249].

This model, titled "Frameworks for International Cyber Security", or "The Frameworks" in short, was first developed on the basis of the expert discussions at the Cyber Conflict Legal and Policy Conference held in Tallinn, September

[249] During 2008–2010, the CCD COE legal experts conducted workshops in Norway, Latvia, the United States and Estonia to discuss views on legal issues and solutions for cyber security.

9–11, 2009.[250] It has been further used as discussion points for expert workshops conducted in the United States, Norway, Latvia, the Netherlands, Finland and Estonia during 2009–2010. This Chapter will introduce, explain and enhance the Frameworks by incorporating additional views and examples in the slide set and integrating additional views and concepts.

2.1. The Spectrum of Cyber Conflict



Depending on the nature and scope of specific threats, cyber security could be regarded as a spectrum where different stages and effects of cyber incidents are aligned. As Westby explains, hard lines between law enforcement and military responsibilities are blurred in the cyber context. An incident may look like an inside event at the outset but, upon investigation, require law enforcement assistance and, within short order, end up being a cyber attack by a nation state in concert with rogue actors.[251]

---

[250] Eneken Tikk. Frameworks for International Cyber Security. First presented at the CCD COE Cyber Conflict Legal and Policy Conference in Tallinn, 9-11 September 2009. Developed over the workshops (*supra nota* 204) and also at the CCD COE Conference on Cyber Conflict in Tallinn, 15-18 June 2010. Original available at https://www.nsm.stat.no/upload/Konferanser%2009/05_Framework%20of%20cyber%20incident_Tikk.pdf (last accessed May 5, 2011).

[251] *Supra nota* 6, page 16.

For the purposes of this dissertation, cyber security is understood as "the absence of a threat either via or to Information and Communication Technologies and networks".[252] Thus, cyber security comprises "cyber defense" as the primarily military responsibility related to preventing, reacting to and mitigating computer network operations, "cyber crime" as the law enforcement's focus area materially covered by cyber crime legal instruments, as well as "information assurance" – the daily routine security concerns related to peace-time functions and purposes of governmental, business and academic networks and information systems.

There are, however, alternative descriptions for the spectrum of concerns posed by the ICT. Professor Denning uses the term "cyber conflict" to characterize different types of threats that have manifested in cyberspace. As Denning summarizes[253], attacks against computers and the data they held emerged already in late 1950s and early 1960s, i.e. long before the Internet was born. Teenage hacking arrived on the scene in the 1970s, andthen grew in 1980s. In 1990s hacking for political and social objectives emerged, blossoming in the 2000s. Now, Denning argues, the latter accounts for a substantial share of all cyber attacks.[254]

Along the popularisation of the Internet, new methods and means of abusing information infrastructure have evolved. While human error has always been a trigger for the incidents[255], cyber crime pursued for economic and personal motivation has developed quantitatively and qualitatively over the past decades. Today, the motivation and reach of perpetrators is no longer only personal or economic – the world is facing an increasing trend of cyber attacks against public and private critical information resources affecting national and global security interests and carrying political and even "perceived public interest" ramifications. Cyber warfare capabilities are reported to date back to early 80-ies in the United States[256] and mid 90-ies in China and Russia, but are only in their infancy in European countries.

The analyses of recent international cyber incidents show that a cyber incident may range anywhere between a simple breach of internal regulations to ideologically motivated or organized cyber crime to national security relevant

[252] Paul Cornish, Rex Hughes, David Livingstone. Cyberspace and the National Security of the United Kingdom. Threats and Responsess. Chatham House: A Chatham House Report. 2009.
[253] *Supra nota* 213.
[254] *Ibid*.
[255] E.g., one of the earliest known cyber incidents is the case of Morris Worm, one of the first worms which was distributed using the Internet, was not intended to cause damage, but to assess the sise of the Internet. However, when Morris, its author, made changes to its spreading mechanism so that it could be installed on more computers, it resulted in unseen volumes of network traffic.
[256] *Supra nota* 6.

cyber attacks.[257] In principle, cyber conflict has the potential to match terrorism and cyber warfare, resulting in casualties and destruction of critical infrastructure and communication.[258]

The cyber conflict spectrum provides a tool for categorising cyber incidents and, in combination with the "Law of Cyber Conflict" spectrum serves as basis for applying and considering the corresponding legal perspective – based on the areas and institutes of law that would be applicable in the case of a particular incident. It categorizes incidents based on potentially applicable legal regimes thus mitigating the observations made by Steven R. Chabinsky, the Deputy Assistant Director of FBI, concludeing that the CNO model broke down as these definitions had no clear legal or policy definition and were never clearly distinguishable in practice.[259]

The current lack of a coherent understanding and diversity of parallel terminology lead to incoherent use of the term "cyber attack" and therefore fail to provide legal clarity as to addressing incidents that took place in Estonia (2007), Georgia (2008), but also Lithuania (2008) and Iran (2010). From the legal point of view, the term "cyber attack" causes confusion since the legal framework for dealing with "attacks" is mainly the one of law of armed conflicts that has few practical impact to the actions taken by Estonia, or Georgia, to defend themselves against the attacks.

The spectrum indicates that every cyber incident needs to be managed and categorised at every stage of its occurrence with potentially different consequences regarding the responses, remedies, and authorities involved. The spectrum thus facilitates the understanding of law and policy makers and those involved in developing cyber security frameworks that the responses to cyber conflict need to reach and cover both ends of the spectrum. It is necessary to analyze the essence and context of an incident to conclude the appropriate response and action. While from a purely technical perspective, cyber incidents may involve similar targets (government websites), methods (defacement, denial of service attacks) and even context (political tensions between two nations), the legal characterisation of such incidents may drastically vary.

The distinctions between the types of incidents represented needs to be tested against individual country practices since, for example, acts criminalised in one country could be subject to internal regulation in others. Clear categorisation of cyber incidents will make it easier to define the authorities responsible for coordinating and managing the incident.

In the Lithuanian case, the defacement of more than 300 websites was made possible by a commonly known vulnerability in one ISP's infrastructure, which could hypothetically have been avoided by better internal auditing of

[257] *Supra nota* 17. Also, Allen D. Walker. Applying International Law to the Cyber Attacks in Estonia. April 2008.
[258] See, e.g., Keith B. Alexander. Warfighting in Cyberspace. – Joint Forces Quarterly. Iss. 46, 2007, pp. 58–62.
[259] *Supra nota* 212, p. 31.

vulnerabilities, which, on the other hand, was not a mandatory procedure under Lithuanian law.[260] Therefore, on the spectrum above, the Lithuanian case could qualify as a flaw of internal regulations that led to a breach of a legal obligation by an ISP towards its customers.

In the Georgian case a month later cyber attacks coincided the Russo-Georgian war thus making the incident potentially subject to applicability of LOAC.[261] However, the cyber aspect of warfare was never brought up by Georgian authorities.

Although some experts consider the cyber attacks against Estonian government servers in 2007 nothing more than a natural outcome of an ill-prepared network defence[262], those who have studied the Estonian information society and the details of the attack can testify that the attacks targeted against Estonia were much more sophisticated than an average, personally or financially motivated intrusion against one single target[263]. As the Estonian authorities had nothing but the Council of Europe's Convention on Cyber Crime-oriented Penal Code provisions[264] at hand for the investigation and prosecution of the 2007 attacks, the only prosecuted person's involvement in the incident qualified as cyber crime[265]. However, the subsequent changes in Estonian criminal law indicate that the next similar incident would be regarded as a national security-relevant act of violence and potentially as cyber terrorism.[266] The Estonian

---

[260] *Supra nota* 17.
[261] *Ibid*.
[262] *Ibid*.
[263] *Ibid*.
[264] Blocking the data in the computer with the purpose of obstructing the work of the computer systemis a crime qualified under the Section 206(2) of the Estonian Penal Code.
[265] According to the judgement of Harju County Court in criminal matter No. 1-07-15185, Dmitri Galushkevitsh wished to express his protest against the activities of the Government of the Republic of Estonia /…/. For this, Dmitri Galushkevitsh used a denial of service attack (hereinafter also DoS attack) in the time period of 25.04.2007–04.05.2007 jointly and in concert with persons not identified during the pre-trial procedure against the server that activates the Reform Party's website, with the intention to obstruct the work of the computer system activating the Estonian Reform Party's website and thereby blocking the services offered by the server (data forwarded by the server) before the other users of the server. To participate in the attack, Dmitri Galushkevitsh repeatedly activated [command] in his place of residence in Tallinn. /…/ Dmitri Galushkevitsh, together with the persons not identified in the pre-trial procedure, by his attack against the computer system activating the Estonian Reform Party's website made it impossible to access the data on the Estonian Reform Party's website /…/, including the Estonian Reform Party's public website /…/ as well as the Estonian Reform Party's intranet activated by the same computer system. In the form of resources spent for prevention of DoS attacks and liquidation of consequences, Dmitri Galushkevitsh /…/ caused damage to the Estonian Reform Party in the amount of EEK 25.210.- and to OÜ E, provider of telecommunications service to the Estonian Reform Party, in the amount of EEK 18.880.-
[266] 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

incident was regarded by the law enforcement and judiciary as cyber crime, but also triggered an amendment of the Penal Code and could these days be qualified as a national security relevant incident.

To sum up, there are different levels of severity, motivation, engagement and effects when it comes to cyber attacks. Often the intent of the intruder can only be determined *post factum* and an intrusion that initially was facilitated by a human error could mutate into wilful and intentional harmful activity that targets not only the enabling information system or infrastructure component, but also those interconnected with it. The challenges related to categorizing cyber incidents and finding the most appropriate responses to them should not be regarded as a reason to give up the categories we have created in our legal and policy frameworks.

Less confusion in the applicable spectrum and a more clear understanding about the potential authorities and remedies involved will facilitate information exchange and help develop more effective remedies over time. More importantly, clear legal categorisation will help to identify the gaps and coordination flaws between the areas of law involved. An important lesson learned from the national security relevant cyber attacks is that in the majority of cases these incidents seem to target the legally less developed areas to escape consequences for the perpetrators.

> "From a legal point of view, given the current and projected future threat environment – increasing threat of asymmetric attacks by non-state entities, less threat of state-sponsored warfare –, there is an increasing likelihood of attacks that fall in poorly defined areas of law. In fact, it is the general murkiness, the lack of clear policies and procedures, the lack of direct evidence of the attacking entity's identity that may make such attacks even more attractive. In such a perceived environment, by deliberately remaining below the threshold of use of force and at the same time using national policy cover as shield against investigations and prosecution, an attacking entity may believe there is less likelihood of reprisal even if the attacker's identity is suspected."[267]

An understanding of the relevance of law in managing cyber incidents will help those involved in incident-handling record the facts relevant from a remedies perspective. Before an incident reaches the threshold of a national security relevant or even armed attack, it could be handled and monitored by a number of institutions. The facts gathered about the origin, duration, technicalities, etc. of the incident may play a significant role in determining a proportionate response in case the attack eventually involves national security authorities and the military.

---

harmonise the Estonian Penal Code with the Council of Europe Convention on Cybercrime and the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, 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.

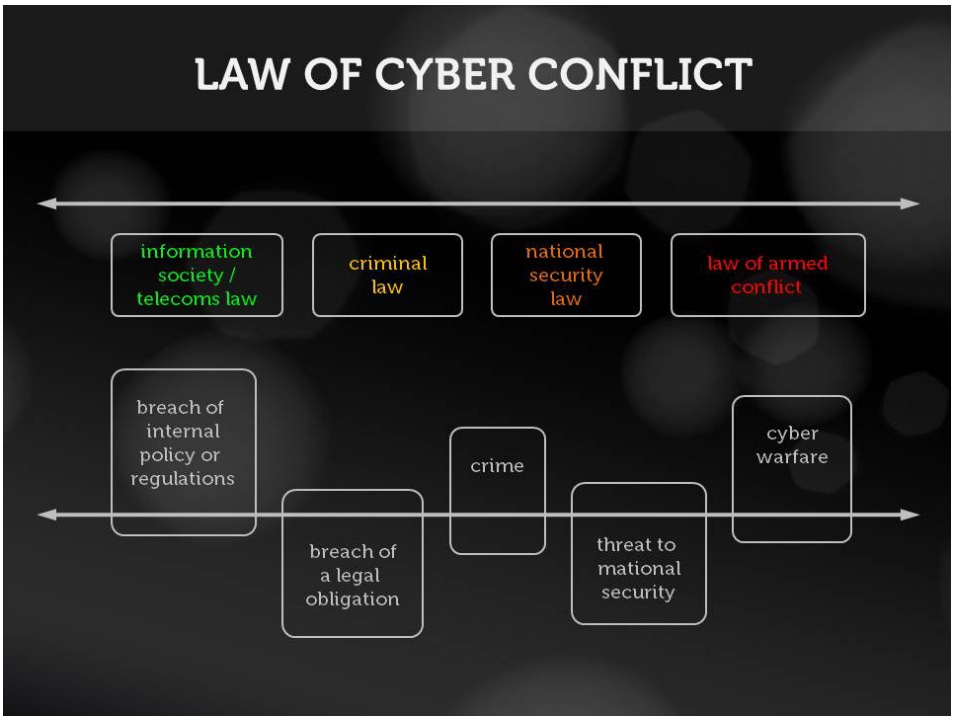
[267] *Supra nota* 17, p. 103.

There will always be a margin of appreciation involved in appropriate defences and responses depending on the attack, method and target involved. For example, while ignoring personal data protection restrictions provided for in law might be tolerated as a "business risk" by some entities and does not necessarily require the involvement of national government once discovered, every intrusion against a critical information infrastructure network is crucial and in case of classified networks, the internal regulation will have to rule out human errors and ignorance. Also, it is impossible to keep track of the "cyber incidents" that occur daily – because there is no single understanding of what constitutes an incident[268] and because there is no single authority or coordinated mechanism to record cyber incidents. And even with a clear definition and an authority in place, we would be talking about astronomical numbers.[269] ideally, at least, each cyber incident has a clear legal mechanism of being handled and categorised at every stage of occurrence – be it a technical measure automatically applied (anti-virus software "killing" a virus, an intrusion detection system reporting an anomaly), human intervention (reporting illegal content) or a response coordinated between national and international entities.

[268] "US Defense Information Systems Agency (DISA) has concluded that Department of Defense (DOD) computers were broken into by unknown persons in excess of 300,000 times in 1994. Indeed, DISA itself tried to test the military's vulnerabilities by hacking into 8,932 DOD computers. /.../ Even more discouraging is the fact that only 4 percent of those hacked into even knew they had been victimised, and, shockingly, only 0.2 percent reported it." – Richard W. Aldrich. The International Legal Implications of Information Warfare. – Airpower Journal. 1996, p. 100. Available at http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf (last accessed May 5, 2011).

[269] Owen Bowcott. "Cyber crime costs the UK more than £27bn a year". – The Guardian, 17 February 2011: Cyber crime costs the UK more than £27bn a year according to a report commissioned by the Cabinet Office into the integrity of computer systems and threats of industrial espionage.

2.2. Law of Cyber Conflict



As explained in the previous section, depending on the motivation, effects and actors, a cyber incident will be categorized as breach of internal regulations, breach of law short of cyber crime, crime, national security relevant incident or cyber warfare. The "Law of Cyber Conflict" slide is intended to explain the legal areas covering the spectrum of cyber conflict. Each of these legal areas (information society/telecommunications law, criminal law, national security law and law of armed conflict has been explored from cyber perspective. [270]

The legal area governing the architecture, setup and security standards of information infrastructure assets can be referred to as IT law, information law[271]

[270] When looking at literature written to address cyber security threats and the legal responses thereto, writings can be easily categorised by the legal background and area of expertise of the authors. Those written from criminal law perspective include, among others, Chik, Broadhurst, Gercke, Goodman. Examples of addressing the issue based on the law of armed conflict background include Schmitt, Wingfield, Denning, Greenberg. Authors falling primarily in the category of cyber law include Wahlgren. A few authors have taken a more overarching view, primarily those addressing the area from critical information infrastructure protection point of view, e.g. Dunn-Cavelty. Also, Susan Brenner, Maeve Dion. Civilians in Information Warfare: Conscription of Telecom Networks and State Responsibility for International Cyber Defense. – Proceedings of ICIW 2010. The 5th International Conference on Information-Warfare & Security, 2010.

[271] A "lighter" version of cyberlaw focusing on the uses and architecture of information. See, e.g., Eneken Tikk, Ants Nõmper. Informatsioon ja Õigus. – Tallinn: Juura, 2007.

or "cyber law" [272]. In general, this is the body of law governing the development and standard of information society services as well as determining the built-in level of cyber security for individual information systems. As Girasa observes, few areas of law have developed so rapidly in so short a time span as Internet (cyberspace) law or cyberlaw.[273] It is interesting to observe that despite the scholarly disputes[274] around the existence of "information law" as a distinct area of law, cyber law has prevailed as a body of law in practice.

Examples of decisive steps taken in the field of criminal law date back to the seventies, but have materialised in national legal approaches primarily since the 1990s, after spreading viruses and sneaking into information systems and databases had become a trend. Portnoy and Goodman observe:

> "Just as the Industrial Revolution created an environment conducive to street or predatory crime through the concentration of the urban population, the Information or Digital Revolution has created a new forum for criminal activity. When the earliest implementations of packet switching networks were first developed by the United States government in the 1970s and early 1980s, certain researchers and computer scientists made substantial initial advances on securing these networks from cyber attacks and malicious exploits. Following a 1983 study on the „possibility of an international application and harmonisation of criminal laws to address the problem of computer crime and abuse", the OECD published Computer-related Crime: Analysis of Legal Policy in 1986. In 1990 the UN adopted a resolution on computer crime legislation, followed by the first important international effort toward developing such a framework in 1992 when the OECD issued Guidelines for the Security of Information Systems and Networks. The aforementioned responses to cybercrime triggered the more intense international initiative to combat cybercrime." [275]

Although criminal law is currently the most exploited legal area of response to more serious cyber attacks, it is not well equipped to deal with large-scale and politically motivated incidents unless it is complemented by policy approaches aimed at national security relevant malicious activities. Increasingly, cyber incidents tend to fall under the less defined legal areas of national (cyber) security and law of (cyber) armed conflict.

As the Estonian incident adequately demonstrated, this traditional prism of cyber crime may not be sufficient to satisfactorily respond to politically motivated cyber attacks. Even if the nation is party to the convention and has implemented its provisions in national law, the functioning of information

[272] The essence and scope of cyberlaw is outlined, e.g. by Gerald R. Ferrera (et al). Cyberlaw: Texts and Cases. – Thomson Publishing, 2nd Ed., 2004.
[273] *Supra nota* 79, p. 3.
[274] Frank Easterbrook. Cyberspace and the Law of the Horse. University of Chicago Legal Forum 1996. pp. 207–216.
[275] *Supra nota* 12.

society and the threats directed against the information society from cyberspace may remain outside the direct scope of its criminal law."[276]

The Law of Cyber Conflict slide illustrates a practical difficulty in reaching coherence in legal analysis regarding cyber incidents as it is a very rare combination for legal experts and advisers to be proficient in all legal areas involved – while coordination between cyber law and criminal law expertise as well as criminal/LOAC expertise are common, attaching the third component to these skill sets is challenging. This has resulted in a stove-piped research pattern – while the military legal community has dealt mainly with information operations and electronic warfare (and used the CNO model as a point of departure), criminal law experts have been busy with new criminal trends like identity theft and credit card fraud and IT legal experts have developed legal policies that consider businesses' best interests with no or little regard to national security interests.

In this context it is understandable how nations and organisations have ended up having not only varying terminology on what in its essence would mean the same thing[277], but, more importantly, similar terminology carrying totally different meanings[278].

Cyber threats today are increasingly targeting information services and systems instead of single entities with different and sometimes combined motivations and various levels of intensity. This slide therefore also emphasises the existing and potential gaps between the legal areas, emphasizing that currently, legal and policy responses developed on both national and international levels do not, *per se*, adequately address a number of cyber concerns[279] and therefore leave a grey area around the categories of and legal remedies to cyber incidents[280]. Understanding and considering different legal perspectives to cyber incident handling will help eliminating gaps and overlaps between legal approaches and, paraphrasing Antolin-Jenkins, 'help finding law in the right place'[281].

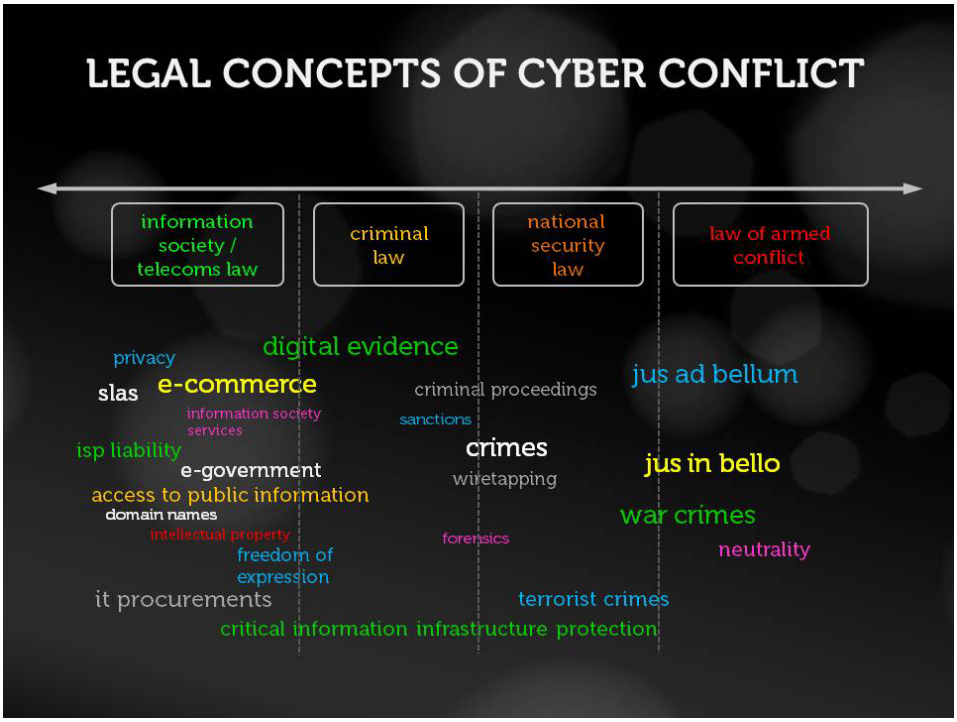
Increasingly, cyber attacks and threats that modern information societies face fall into the area of national security law that is the regulatory prerogative of nation states and therefore is not clearly delineated on the international level. One can find examples of national security-related exceptions in international legal instruments that, based on national interpretations, will form a separate body of law on the national level. For example, according to Article 19 (1) of

[276] *Supra nota* 17, pp. 99–100.
[277] For example, the EU countries widely use the term "network security" in the same context that the US increasingly uses "cyber security".
[278] For example the inconsistent use of terms like "cyber attack", "cyber defense" etc. in national cyber security strategies, policies and legislation.
[279] Such as newer criminal trends (e.g. phishing, cyber espionage), cloud computing, responsibility for incidents in case of insufficient attribution etc.
[280] Chapter III of this dissertation will further elaborate on this.
[281] *Supra nota* 8.

the International Telecommunications Convention[282], nations have the right to stop the transmission of any private telegram which may appear dangerous to the security of the State. Pursuant to Article 9 (2) of the Council of Europe Data Protection Convention, exceptions to the provisions of Articles 5, 6 and 8 of it are allowed when "provided for by the law of the Party and [when they] constitute... a necessary measure in a democratic society in the interests of protecting State security".[283]

Therefore, legal responses and remedies to incidents and stages thereof may derive from different legal areas that have different reach and limitations under domestic legal systems and approaches. Recognizing this will improve understanding about potential remedies available and better coordination between legal scholars and practitioners with different expert background.

2.3. Legal Concepts of Cyber Conflict



With different areas of law involved in cyber security, the legal concepts involved in cyber incident handling need to be developed, applied and

[282] International Telecommunication Convention. Concluded at Nairobi on 6 November 1982.

[283] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.1981.

interpreted in a coherent manned to achieve efficient coordination between legal areas. Concepts such as e-commerce, IT procurements, freedom of expression, privacy and others are so far primarily regarded as belonging to the area of the regulation (and implementation) of information society law or cyber law. Cyber crime law combines elements of computer crime and relevant procedural aspects whereas the Law of Armed Conflict is intended to define the threshold and framework of military responses to cyber incidents.

From a regulatory perspective, it is essential to look at these legal areas in a systematic and coherent way to identify related concepts and possible areas of confusion. An example of a legal concept regulated from different perspectives is the one of "data" which from an information society law perspective focuses on personal data protection, potentially turns into evidence in the context of criminal law and is regarded as intelligence or mission planning information in the context of national security and military responses. Thus, "data" is subject to regulation of, e.g. EU and COE data protection instruments, the Cyber Crime Convention, but also the Geneva Conventions.

It is necessary to bridge the regulation and legal practices in the areas indicated above to achieve a comprehensive legal approach to cyber security. As of today, publicly known advances in information technology have primarily been developed by individuals or companies for commercial purposes. This explains why defences designed for individually owned and operated ICT assets often fail when confronted with a large-scale, politically motivated or terrorist cyber attack. From a business perspective, investments into the security of information systems take into account the projected quantity of customers and volume of use, as well as the technical specifications of services rendered to the users. Business entities cannot be expected to have sufficient incentive to invest into network and service security beyond the level of their own sustainable business interests and anticipated return. The collective risks of other market players are normally not calculated into the investment formula of a single enterprise. The role of coordination of "collective defenses"[284], as well as that of minimisation of collective risks, is that of the governments."[285]

The European Union, which has more than two decades of experience of developing a strong legislative base for information society, IT and electronic communications law, has, until recent years, largely refrained from the cyber security and cyber defense debate. The exclusion clauses contained in EU law, which preclude the applicability of EU law in the areas of public security and criminal law, have also caused the public and political pressure to be far more aligned towards individual freedoms than public security. In addition, privacy law and other legal areas related to individual freedoms are much more homogeneous and transparent thanks to the systematic harmonisation efforts. Yet even though security is still an area where EU institutions do not exercise

[284] This term should not be confused with the notion of collective self-defense in international law.
[285] *Supra nota* 17, p. 97.

legislative authority even after the entry into force of the Lisbon Treaty, this does not preclude intergovernmental cooperation among EU member states in harmonisation of national cyber security approaches.[286]

So far, many legal concepts of huge relevance to cyber crises (cooperation between authorities and ISPs, quality of data available about the incident etc.) are by default developed with market interests and incentives in mind[287] and thus often directly contradict the expectations of crisis management entities in case of an incident involving more than one entity as target. There is an increasing amount of information available about politically motivated and government-targeted cyber incidents. The management of cross-border cyber incidents and conflicts, however, requires extensive and detailed information-sharing among governmental entities and also among these last and the entities responsible for the information infrastructure, which are often privately owned. This kind of cooperation is inevitable between nations and international organisations. The data of interest comprises not only details about the course of action and background of the incidents but also real-time reporting on targets and, most importantly, details of the server logs, which make it possible to differentiate the good traffic from the bad, block hostile IP addresses, and trace the origin of the attacks. /…/ While the [EU and NATO] share interest in the field of Critical Infrastructure Information ("CII") protection, personal data protection in the EU legal framework may become a factor that could hinder the creation of effective cyber defense, unless timely and duly attended to by the interested nations and entities. There seems to be some inconsistency in the application of the Directive 95/46/EC (herein after referred to as 'the Directive' or 'the 'Personal Data Protection Directive') by the Member States. These differences in interpretation and application of the Directive are particularly evident when looking at the approach of Germany in comparison with Sweden. These two cases will be discussed below. Yet, the dominant view held by the EU data protection authorities require information sharing regarding cyber incidents be supported by specific legal provision under national law."[288]

The situation gets particularly complicated in case interoperability and cooperation is needed between two or more countries. While, for example, within the EU countries, one can expect similar legal understanding about issues such as preserving log files, exchanging incident data and relying on ISP cooperation, the situation changes drastically as soon any third countries become involved. In the context of information exchange regarding cyber

[286] *Ibid*, p. 100.

[287] For example, the aim of the EU (in addressing e-commerce in Directive 2000/31/EC) is to remove legal barriers which could impede the spread of electronic services across Europe. The aim of the Data Protection Directive is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data (Article 1 (1).

[288] See Eneken Tikk. Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective. In Modelling Cyber Security: Approaches, Methodology, Strategies. NATO Science for Peace and Security Series, Vol 59. Amsterdam: IOS Press.

attacks, one of the more important provisions of the EU Data Protection Directive in the context of exchange of information about cyber attacks is Article 25, which prohibits the transfer of personal data to third countries.[289]

With regard to jurisdictions with a lack of incentive and preparedness to cooperate, cyber attacks are a convenient coercive measure with uncoordinated and sometimes lacking legal responses.

Therefore, any regulatory measures and responses to cyber incidents need to be considered from at least four different legal perspectives – information society development and private investment incentives, law enforcement and cross-border as well as inter-agency cooperation and coordination in case of international security concerns and ultimately, coordination on national and international peace and security. The level of confidentiality, integrity and availability built into critical information services and systems in peace time will pre-determine the available defences in case of a wide-scale cyber attack. Although from a technical point of view, adding resources in case of an emergency could be possible, differing policy priorities and a lack of regard to legal obligations can stand in the way of effective defence. As an example, the electromagnetic spectrum is a finite resource, and as it is sold off for commercial uses with no regard to potential crisis-handling requirements, it may force [the military] to operate on suboptimal frequencies in case of a national security relevant incident. This could jeopardise missions of security relevance. It is also known that during the Kosovo campaign the aerial refuelling operations were affected by failure to coordinate a new refuelling navigation system; intelligence operations had to be curtailed because of the possibility of interference from neighbouring countrys' commercial broadcast signals.[290]

As explained in the context of recent international cyber incident analysis, it may not be the best tactic to focus on defining whose area of responsibility a particular type cyber attack might be – whether it is "an IT security problem" or "a law enforcement problem" or "a military problem". A national-scale cyber

[289] The Member States shall provide that the transfer to a third country of personal data, which are undergoing processing or are intended for processing after transfer, may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectorial, in force in the third country in question and the professional rules and security measures which are complied with in that country.

[290] Report of the Defense Science Board Task Force on DoD Frequency Spectrum Issues Coping with Change: Managing RF Spectrum to Meet DoD Needs. Defense Science Board. Washington: 2000. Available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA386136&Location=U2&doc=GetTRDoc.pdf (last accessed May 5, 2011).

attack is a problem affecting the society – its security and public order – as a whole."[291]

Therefore, as a first step, the development of an information society needs to be backed up with legal protection of privacy, freedom of speech, consumer rights and other "practical" aspects of a well-functioning peace-time information community. Realising however that the desired harmony needs to be enforced against cyber criminals, nations need to modernise their crime law – both procedural law and substantive criminal law to make sure that the gaps in procedure do not affect implementation of penal law (as we partly saw it in the Estonian case). Also, having in mind the vulnerability of vital information systems and command and control functions, one also needs to prepare for cyber war from a legal perspective already when developing policies for general information architecture and network security."[292]

Over the past decade, a new legal concept has developed that helps frame the critical assets from a cyber security perspective and potentially could be reflected on the slide. Dunn Cavelty explains that objects whose incapacitation or destruction would have a debilitating aspect on the national security and the economic welfare of a state are referred to as critical infrastructure (CI).[293] The list of such objects differs by nation, but frequent examples include telecommunications, power grids, transport and storage of gas and oil, banking and finance, traffic, water supply, emergency rescue services and public administration.[294] The Estonian Cyber Security Strategy lists nine categories of critical infrastructure.[295]

While military supplies and assets are usually regarded as objects subject to national security legislation scope of protection, the legal framework of protecting CI is less distinct. In its essence, protection of CI cannot be limited to one legal area, as CI has functions that cannot be distinguished as purely private or public, civil or military. This poses a significant challenge to legal experts as

---

[291] *Supra nota* 17, pp. 103-104.
[292] *Ibid*, p. 104.
[293] Myriam Dunn Cavelty. Critical Information infrastructure: Vulnerabilities, Threats and Responses. – Geneva: United Nations Institute for Disarmament Research, 2007, p. 16.
[294] *Ibid.*
[295] Energy facilities and networks: electricity, oil and gas storage facilities and refineries, transmission and distribution systems; Communications and information technology: telecommunications, transmission and notification systems, software, hardware and networks, including the infrastructure of the Internet; Finance: banking, securities and investment; Health care: hospitals, health care facilities, laboratories and medicines, search, rescue and ambulance services; Food: safety, means of production, wholesale and food industry; Water: water reservoirs, water treatment plants and water networks; Transport: airports, ports, inter-modal transport facilities, rail and mass transit networks, traffic control systems; Production, storage and transport of dangerous goods: chemical, biological, radiological and other hazardous materials; State agencies: critical services, facilities, information networks; information systems ensuring national security and defense, resources, databases and court registers with legal effect, and national cultural assets. *Supra nota* 102.

the traditional legal approach has been to distinguish between economic well-being and national security as legally protected values.

Critical infrastructure assets in a modern society are either based on or monitored and controlled by ICT systems. Therefore protection of CI nowadays heavily relies on security of information infrastructure (CII).[296] In the CII context, economic well-being and national cyber security are closely interconnected, since CIIs are essential for both dimensions at the same time.[297]Thus, legal framework of CI protection is a combination of remedies available under different legal areas.

CII therefore forms a dimension of cyber security, determining objects, processes and functions that need to be secured consistently through all legal areas. Unlike many user- and public-oriented functions and services, CII needs to be backed up with effective legal remedies sufficient to create a deterrence shield around it.

CII as a legal concept is overarching, falling into several legal areas simultaneously. Of course, depending on the area involved, the scope and methods of protection differ – e.g. LOAC legal remedies will be available in case CII falls under an armed attack and from a personal data protection perspective, CII attacks could just present an exception from routine data exchange procedures.

The threats to CII are multi-faceted and may have different motivations and a wide spectrum of potential perpetrators. Thus, an incident involving CII objects might be an accident, a human error, the outcome of a curious teenager hack, well-planned and targeted intrusion with fiancial purposes, a widely coordinated politically motivated intrusion or part of the plan of an armed conflict.

Therefore, CII protection does not form a separate legal area, but rather a layer of additional protection that needs to be considered when developing systems and services critical for society's functioning. The proposal made by Ms. Maeve Dion at the Cyber Conflict Conference to place the critical information infrastructure protection concept to overlay all three legal areas involved is being taken into account when developing this slide.

[296] *Supra nota* 102, p. 17.
[297] *Supra nota* 102, p. 8.

2.4. Areas of Cyber Incident Management

The concern of lawyers not being able to understand and keep up with the development of technology has accompanied legal scholarly work from the early phases of Internet regulation. Easterbrook,[298] Katsch[299], Reidenberg[300], Grimmelmann and Ohm[301], Manolopoulus[302] and many others observe that in the information society, legal analysis and legislative drafting needs to take into account the development and use of the underlying technology itself. With the growth of cyber incidents of both cross-border and political nature, legislation, legal interpretation and analysis also needs to be linked to professional practices of diplomacy, intelligence, military, policy and economics to redefine and, where necessary, set a new balance to current legal instruments and practices.

The "Areas of Cyber Incident Management" slide is based on a concept presented by Professor Thomas Wingfield in a workshop in 2008[303]. The DIMPLE standard proposed by Prof. Thomas Wingfield suggests that since

[298] *Supra nota* 274.
[299] Ethan Katsch. Cybertime, Cyberspace and Cyberlaw. 1995 J. Online L. Article 1.
[300] Joel R. Reidenberg. Lex Informatica: The Formulation of Information Policy Rules Threough Technology. Texas Law Review, Volume 76, N0. 3, February 1998.
[301] James Grimmelmann, Paul Ohm. Review of The Future of the Internet – and How to Stop It by Jonathan Zittrain. 2009.
[302] Andreas Manolopoulus. Raising Cyber-Borders: The Interaction Between Law and Technology. International Journal of Law and Information Technology, Vol. 11, No. 1.
[303] Workshop on Cyber Law at the CCD COE on December 8-9, 2008.

cyber incidents handling requires a constructive debate among experts from different areas, the events need to be described in a manner allowing experts of all relevant fields (Diplomacy, Intelligence, Military, Policy, Law, Economy) to understand the situation. This promotes discussion in the field and would ideally avoid parallel vocabulary and misunderstanding on the topics of common concern.

The DIMPLE construct would allow decision makers in any given area to access the body of information from a perspective that includes as much relevant, and as little irrelevant, information as possible. [304]

Therefore, law is but one aspect and tool for cyber incident handling. Developing Wingfield's idea further and combining it with the critique towards the ability of lawyers and the regulatory framework to have regard to technology, the author of this dissertation would argue that the role of law and lawyers should primarily be regarded as "mission support" to other cyber incident handling roles. In the context of a comprehensive approach law is just one area of expertise and one set of instruments to be applied in order to achieve wide-base coordination and mitigation of cyber security.

It is therefore essential that legal issues related to cyber security are defined, elaborated and responded to in an interdisciplinary manner, combining the observations, conclusions and methods of all arenas involved in managing cyber security in different stages and on different levels.

[304] Thomas C. Wingfield, Eneken Tikk. Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen. – International Cyber Security Legal and Policy Proceedings, CCD COE Publishing, 2010.

2.5. Levels of Cyber Incident Management

With all possible means, targets, actors, effects and defences, cyber security may look like a mission impossible from every single stakeholder's point of view. The best platform of defence is therefore created by a combination of perspectives and approaches.[305]

The "layers" of implementing cyber security involve a wide variety of stakeholders whose tasks and authority are interrelated. Essentially, four levels of cyber incident handling involvement can be distinguished.

Due to the growing trend in past years of incidents with a political context, cyber security has reached the attention of larger international organisations. An intensive discussion about the need for additional instruments on the international level is going on.[306] At the same time, the conclusions of Schmitt still hold – with the current digital divide and differing cyber security concerns, the international community *en large* is not yet ready to adopt fundamental decisions about global cyber security.[307]

On the international level, organisations such as the Council of Europe, the European Union and G8 are qualitatively in a position to adopt legislation that would coordinate responses to cross-border cyber incidents. Quantitatively,

[305] COL Ilmar Tamm. Introduction. – International Cyber Security Legal and Policy Proceedings, CCD COE Publishing, 2010.
[306] *Supra nota* 15, 16.
[307] S*upra nota* 26.

however, these organisations only cover about 1/3 of the countries in the world, whereas shopping for convenient jurisdictions has been and remains an option for perpetrators.

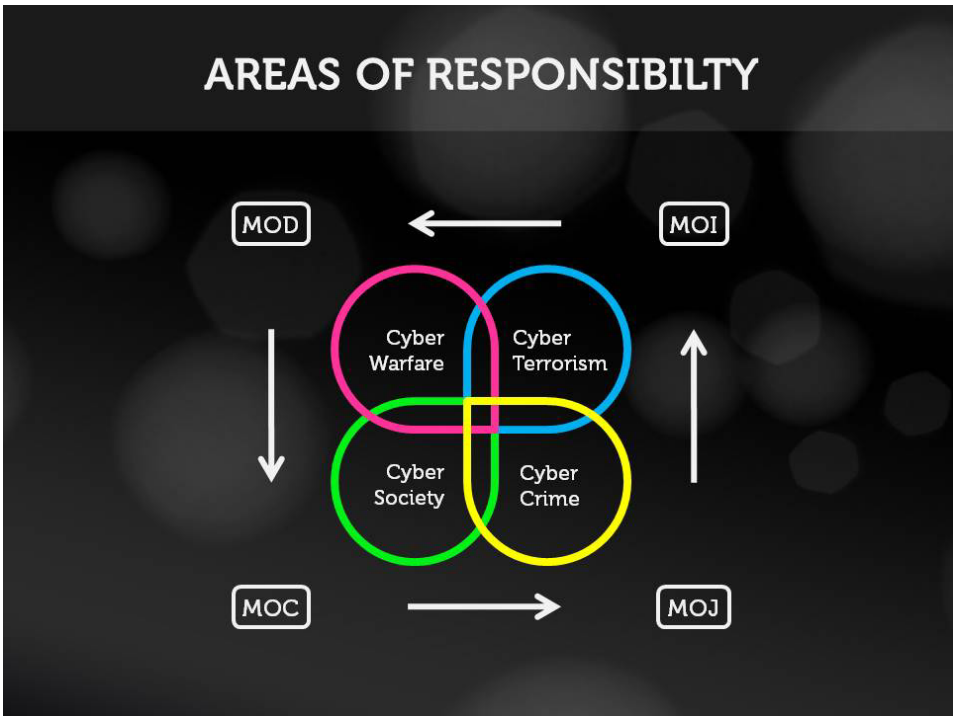
Efforts on the national level need close coordination in terms of public and private sector involvement. As the Estonian case showed, cyber security needs to be balanced between different areas of authority to allow for coherent planning and coordination of remedies and defences. The interaction between areas of responsibility based on the Estonian authorities' model is reflected on the slide "Areas of Responsibility". Put in another country's context, the division authority may differ in terms of the institutions involved, but not too much in terms of functions covered.

Given the divided and diffuse focus of international organisations, the primary responsibility for addressing cyber security threats and responses currently lies with national governments. Without a thorough understanding of threats and remedies available on the national level any debate on the international level would lack focus. Only after national homework can the areas for common concern be referred to in detail sufficient for constructively debating additional remedies needed.

Coordination between the public and private sectors is one of the challenge areas since, given the information infrastructure architecture in place, there is no effective way for governments and the military to achieve the required level of security without private sector involvement.

At the level of individual users, the impact of this on the ability of the governments and international organisations to implement their policies and regulations is difficult to overestimate. The large community of users does not "fit" into the area of authority of any particular international organisation or government and therefore engaging this community in the defence of national security interests can only occur with the help of the industry and service providers. With coercion and enforcement being essential elements of the legal order, states therefore need to be careful when imposing security-related obligations on end users that may be practically impossible to supervise by national authorities.

2.6. Areas of Responsibility



Because of the wide spectrum of threats and accordingly, defences, there is no single area or point of authority in charge of cyber security. As Aldrich summarizes, cyber warfare is not only the concern of the Department of Defense or its equivalent. Defense in cyberspace is also about the ability to fight computer crime, which involves the Department of Justice. It is about computer security that in the United States is the area of responsibility of the National Institute of Standards and Technology, in Europe more likely of Ministry of Economics and/or Communications. It is about intelligence gathering that is the concern of intelligence agencies and about national security that belongs to the area of government of the Ministries of Internal Affairs. [308]

Estonia was one of the countries to develop an information society strategy that implemented the EU information community agenda.[309] Until 2007, the

[308] Richard W. Aldrich. Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime. US Air Force INSS Occasional Paper 32. April 2000.

[309] The preface of the information policy principles adopted in 2004 explains: "[Estonian] IT policy follows the objectives set out in the eEurope 2005 action plan and other strategic documents in Europe. Thus, the priority fields of the eEurope 2005 action plan – e-services in eGovernment, eLearning, eHealth and eBusiness as well as their secure underlying infrastructure – are the key words of the Estonian information policy." – Supra nota 19. The introduction to the Estonian Information Society Strategy 2013 states: "Activities to be

Estonian information policy had been primarily shaped by the Ministry of Economics and Communication. The development policy of the information society between 1998 and 2003 was based on the Principles of Estonian Information Policy[310], adopted by the Estonian Parliament. In 2004, Principles of the Estonian Information Policy 2004–2006: Towards a More Service-Centered and Citizen-Friendly State were enacted[311] and in January 2007, the Information Society Strategy 2013 entered into force.[312]

The legislation in the field has been co-developed by primarily the Ministry of Economics and Communication (the authority also responsible for implementing the EU information society agenda) and the Ministry of Justice. The legislative framework, however, has been driven primarily by the growing demand for ICT solutions as well the interests of ICT sector competitiveness.[313]

In 2006, a study was prepared upon the request of the Estonian Ministry of Defence to evaluate the cyber defence capabilities of the Republic of Estonia.[314] The analysis document indicated weak coordination and different perceptions of vulnerabilities and required defences by Estonian private and public sector authorities. It also revealed that no clear definition of critical information infrastructure existed in Estonia and that based on the authority statements, gaps

---

carried out in the framework of the strategy are in line with the priorities set out in the Estonian Action Plan for Growth and Jobs 2005–2007 and the Estonian National Development Plan for the Implementation of the EU Structural Funds 2007–2013. In addition, the strategy is mutually complementary with several other sectoral development plans, such as the Estonian Enterprise Policy 2007–2013, the Estonian R&D strategy "Knowledge-Based Estonia 2007–2013", the Strategy for the Preservation of Estonian Digital Heritage 2007–2010 etc." – Estonian Information Society Strategy 2013. 2006, p. 4. Available at http://www.riso.ee/en/system/files/Estonian%20Information%20Society%20Strategy%202013.pdf. Neither of the documents sees cyber security as one of the key challenges of implementation.

[310] Principles of Estonian Information Policy. Estonian Parliament, 1998. Available at http://www.riso.ee/en/files/Principles_of_Estonian_Information_Policy_1998.pdf (last accessed May 5, 2011).

[311] *Ibid*.

[312] *Ibid*.

[313] A policy statement by the Estonian Informatics Centre explains: "[t]he development of the information society through the creation and application of IT solutions (the state information system, the administration system for the information system (RIHA), the X-Road, portals, ID card applications, Electronic Health Record, ID ticket etc), the growing demand for innovative solutions as well as the increasing need for borderless Europe and world have started a process, which calls for the establishment of ever clearer rules of conduct and decision-making." – ICT legislation in Estonia. Available at http://www.ria.ee/public/publikatsioonid_/ICT_legislation.pdf (last accessed May 5, 2011).

[314] This was the first task of the Project Team for the Cooperative Cyber Defense Centre of Excellence. Under the lead of Prof. Peeter Lorents, the team of 6 experts conducted a study from May to October 2006.

and overlaps in authority to develop cyber security solutions for national information systems and responding to major cyber incidents.[315]

The 2007 incident was handled *ad hoc* under the supervision of the Estonian Ministry of Defence whereas the practical role of the Ministry of Economics and Communications was limited to the involvement of CERT-EE. A working group was created by the Minister of Defence in 2007 to analyze the incident and propose ways to improve the cyber security preparedness in Estonia. The working document of the expert group served as input for the Estonian Cyber Security Strategy adopted in 2008.

The strategy saw enhancing inter-agency co-operation and co-ordination in ensuring cyber security and continuing public and private sector co-operation in protecting the critical information infrastructure as some of the key objectives in developing and implementing a system of security measures.[316] It proposed a number of measures for better coordination of cyber incident handling, proposing that supervision of the implementation of security measures for the critical infrastructure would be conducted by the Ministry of Internal Affairs and the Ministry of Economic Affairs and Communications in co-operation with other ministries responsible for different sectors of the critical infrastructure[317]. The responsibility for developing the "Implementation Plan for Cyber Security Strategy 2008–2010" was imposed to the Cyber Security Strategy Committee, led by the Ministry of Defence in co-operation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs, the Ministry of Foreign Affairs and private sector representatives.[318]

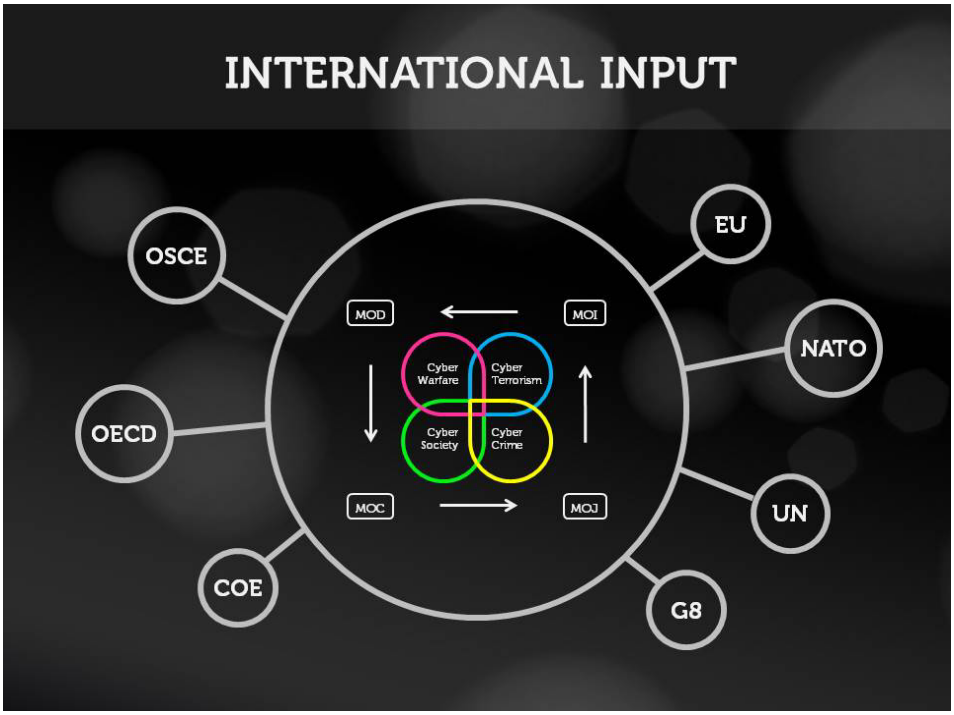
Estonia is not the only country that has introduced a new model of cyber security organisation and recognised the need for combining institutional approaches to protect the information society. In the Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space of 2009, the UK Government has expressed their intent to "establish an Office of Cyber Security (OCS), that will initially be set up in the Cabinet Office. The OCS will have overall ownership of the Cyber Security Strategy, will provide strategic leadership across government for cyber security issues, and will drive delivery of the Strategy through a cross-government programme, elements of which are already underway, for example in the Information Assurance field under the National Information Assurance Strategy".[319] The Strategy to improve Internet Security in Sweden (2006) takes an even wider approach to the cyber security

[315] Peeter Lorents, Enn Tõugu, Risto Vaarandi, Toomas Kaevand, Jüri Kivimaa, Eneken Tikk. Cyber Security Situation in Estonia. – Estonian Ministry of Defense, 2006. Document with restricted access.
[316] *Supra nota* 102.
[317] *Ibid*.
[318] *Ibid*.
[319] *Supra nota* 103.

structure and lists international and Swedish organisations that are relevant to Internet security.[320]

While the names and distinct lines of authority differ by country, the trend moves towards a cross-governmental approach to national cyber security that would define and cover the whole spectrum of information society development, exploitation and defence issues. This way, measures designed to create a more competitive and convenient information society for users would be balanced and combined with national cyber threat assessment concerns as well as planned in a manner satisfying the potential needs of law enforcement, intelligence and military. The Areas of Responsibility slide visualises this trend and serves as a reminder to coordinate cyber security efforts between all relevant national authorities in order to avoid overlaps and gaps in prevention, detection and response.

2.7. Links Between International and National Legal and Policy Instruments



[320] Strategy to improve Internet security in Sweden. 2006, pp. 59-67. Available at http://www.pts.se/upload/Documents/EN/Strategy_Internet_security_2006_12_July_2006.pdf (last accessed May 5, 2011).

The "International Input" slide explains how international organisations' approaches potentially shape and influence national development and implementation of cyber security strategies and regulations and accordingly, what needs to be implemented by nations depending on their membership in particular organisations.

With the cyber security strategic planning focusing on developing more widely accessible services and supporting the growth of e-commerce and social networking, national authorities responsible for economics and communications have served as the counterparts for implementing EU information society directives and action plans. Ministries of telecommunications (or their equivalents) have traditionally been responsible for ensuring the quality and security of communications services and infrastructure, primarily deriving guidance from the EU, OECD and UN WSIS. Law enforcement and justice authorities have jurisdiction over national applications for EU activities in the area of freedom, security and justice as well as over various cyber crime instruments. The fight against terrorism as well as the management of national security relevant incidents is typically handled by the Ministry of Interior or its equivalent. Thus far, there is no publicly known information involving terrorist attempts to compromise or disable information networks or to execute operations with physical effects. But one cannot rule out the possibility that such intentions or capabilities may emerge in the future (OSCE, UN). Under some circumstances, a disruptive activity using ICTs could constitute an armed attack and potentially invoke the right to collective self-defence. A response to a cyber attack crossing the threshold of an armed attack falls under the purview of the military and ministries of defence. Although the Estonian attacks in 2007 cannot be regarded as a valid example of a "cyber armed attack," military authorities around the world have become more actively involved in strategic cyber security planning after the incident. Individual and collective self-defence in case of a cyber armed attack is subject to coordination between the UN, NATO and national authorities responsible for the military domain.[321]

Based on these observations, having regard to the nature and current setup of the information society and in conjunction with the study of recent national strategic approaches to cyber security, one can conclude that the structure of cyber security legal and policy measures comprises different stakeholders, levels of intervention, methods of prevention, detection and response, as well as hierarchies of decision-making and guidance. A comprehensive structural approach to cyber security therefore needs to consider all relevant legal areas, levels of regulation and concepts.

[321] *Supra nota* 146.

CHAPTER III.
INSTRUMENTAL LEGAL FRAMEWORK FOR INTERNATIONAL CYBER SECURITY

Introduction

The need for new rules on Internet Governance and cyber security has been advocated by several international organisations over the past decade. The discussions in the Council of Europe, UN and OSCE have led to attempts to generate a framework for directing the behaviour of different stakeholders. The inadequacy of the existing legal framework to support cyber security efforts has also been pointed out by national representatives as one of the key challenges to effective cyber defence and security: The current regulatory and legal environment hinders cyber security by imposing overly prescriptive regulations while failing to fill troublesome gaps in the legal and policy framework.[322] A growing *Mindermeinung*, however, is that international law and cooperation as they exist are enough to tackle cyber security issues for now.[323]

A deeper look into different proposals on how to overcome the gaps and inconsistencies in the current legal framework indicates disparity between methods of achieving regulation that corresponds to the current cyber security paradigm. The observation made by Sklerov refers to three different ways of approaching the issue. Sklerov concludes that state responses to cyber attacks are governed by an anachronistic legal regime that impairs a state's ability to defend itself. No comprehensive treaty exists to regulate international cyber attacks. Consequently, states must practice law by analogy. [324]

As follows from Sklerov's conclusion, there are potentially three ways to overcoming the legal inconsistencies that inhibit cyber defence efforts. The first of the three is the application of law by analogy proposals made by Hollis, Geers, Kamal, and Schackelford. The second relates to new treaty law proposals (Hughes, Hollis, Ghernaouti-Hélie, Schjolberg).

The author has decided on the third way, which supports the minority opinion that the existing legal framework is sufficient for resolving most cyber security related legal problems. In taking an interdisciplinary analytical

---

[322] Among others Senator Carl Levin (Chairman of US Senate's Committee on Armed Services), Gen. Keith Alexander (Head of U.S National Security Agency and US Cyber Command), Jaak Aaviksoo (former Minister of Defense of the Republic of Estonia), Nick Harvey (UK Armed Forces Minister). See, e.g. National Cyber Security Research and Development Challenges, I3P, 2009. Available at http://www.carlisle.army.mil/DIME/documents/i3pnationalcybersecurity.pdf (last accessed June 25, 2011).

[323] Among others Christopher Painter (Coordinator for Cyber Issues for the US State Department).

[324] Matthew J. Sklerov. Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent. – 201 MIL. L. REV. (1-85) 2009.

approach to existing legal frameworks and with reference to the analysis of existing international legal instruments and recent state practice in resolving cyber incidents, the author concludes that there is no immediate need to apply law by analogy to cyberspace activities as the quantitative analysis underlying this dissertation has identified more than 30 legal instruments adopted by international organizations that cover the cyber security spectrum. With reference to Hollis and others, the author also shares the view that the law, by analogy, will not increase certainty and uniformity among states, courts and international organizations about international law. As regards the treaty approach, the author sees the proposed conceptual approach of this dissertation as an interim step towards concluding which aspects of cyber security require additional regulation on the international level.

There have been numerous occasions in history when law and legal interpretation have been revised due to extensively changed circumstances, without new treaties being adopted on internationally. One of the best-known occasions is the aftermath of the 9/11 attacks that led to restatements in the law pertaining to the use of force, state responsibility, privacy and several other legal concepts.

With reference to the conclusions above, this chapter will argue that before applying any analogies, one should look into already existing regulations that are designed with different elements of cyber security in mind or reflect generally accepted legal principles that can be applied to cyber space. Taking a closer look at already existing international legal and policy frameworks, most legal constructs we need to tackle cyber security issues exist under international law, although scattered around different instruments of different scope and often in need of cross-disciplinary interpretation according to the contemporary threat context.

There are indications of the need for revision of current interpretation and implementation practices in virtually all legal areas dealing with cyber security. As Vogel explains, there is no universally accepted definition of cybercrime as such. […] Accordingly, the scope of specific cyber offences is not limited to manipulating or sabotaging computers. Rather, modern cyber offences relate to a variety of harmful behaviors involving information systems and/or data […].[325]

Sklerov explains that with deterrence coming from criminal law, the failure of states to pass stringent criminal laws or their tendency to look the other way when attackers strike rival states will render criminal laws impotent.[326] There might be other flaws in the criminal law framework that require restatement of existing legal interpretation and potentially the legal instruments. As noted by Chic, existing legislation may not be suitable or adequate, since the language in criminal statutes may not apply, jurisdictional issues may arise and punishments

[325] *Supra nota* 136, p. 1-2.
[326] *Supra nota* 324, p. 9.

may not be appropriate.[327] Gercke suggests that regular updates are relevant not only with regard to substantive criminal law, but also with regard to procedural law, as new technologies and practices require further attention in considering whether amendments in the legal framework are necessary.[328]

Streltsov observes that there are no such concepts as national border and territory in the information sphere[329], thereby hinting that new legal concepts need to be developed for this global phenomenon. Condron adds that the problem with the concepts of defence and security is that they rely on the concept of geographical borders, which are almost meaningless in cyberspace because cyberspace has no borders or boundaries in the traditional sense.[330]

As observed by Antolin-Jenkins, translating essential terms of self-defence legal propositions into application in cyberspace is in its embryonic state and requires defining what constitutes an armed attack in cyberspace, what acts can be taken in self-defence and what constitutes a proportional response.[331] Sklerov notes that the current legal paradigm, which requires attribution to a state or its agents, perpetuates the response crisis because it is virtually impossible to attribute a cyberattack during an attack and that the "attribution problem locks states into the response crisis".[332]

As Grief explains, the European Court of Justice has repeatedly annulled decisions related to the transfer of personal data by EC air carriers to US authorities because data processing operations which concern public security and/or the activities of the state in areas of criminal law are excluded from the scope of the [Data Protection] Directive and fall outside of the scope of Community Law. [333] At the same time, the prevailing view in the data protection legal community is that IP addresses are personal data and therefore subject to the Directive.

Last but not least, the nature of cyber conflict is still evolving. Geers notes that the real-world impact of cyber conflict is still difficult to appreciate, in part because there have been no wars between modern, cyber-capable militaries.[334] Denning explains that cyber conflict is an emerging social phenomenon in terms of social networks of non-state warriors launching cyber attacks for social and

---

[327] Warren B. Chic. Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore, 2007. – Research Collection School of Law. Paper 348. http://ink.library.smu.edu.sg/sol_research/348

[328] *Supra nota* 71, p. 419.

[329] A. A. Streltsov. International Information Security: Description and Legal Aspects. In: Disarmament (Vol. 3), 2007

[330] Sean M. Condron. Getting it Right: Protecting American Critical Infrastructure in Cyberspace. Harvard Journal of Law & Technology. Volume 20, Number 2, Spring 2007, p. 409.

[331] *Supra nota* 6.

[332] *Supra nota* 324, p. 7.

[333] Nicholas Grief. EU Law and Security. – E.L.Rev. 2007, 32(5), 752-765.

[334] Kenneth Geers. The Challenge of Cyber Attack Deterrence. – Computer Law & Security Review March, 2010. doi:10.1016/j.clsr.2010.03.003.

political reasons.[335] New rights have been generated by national judiciaries and legislatures to support the new way of life surrounding the development and sophistication and widespread use of information and communication technologies.[336]

While flaws and gaps exist in the current legal framework surrounding cyber security, the lack of precise definitions of means and remedies to combat cyber threats is not necessarily an indication of the need for new legislation.

Streltsov brings an example related to international law concerning the maintenance of international peace and security, observing that the UN Charter establishes a universal mechanism for maintaining it. He suggests that with the development of ICTs the Charter could be interpreted in such a way as to provide international actions with a considerable degree of freedom to use ICTs to take aggressive actions and solve international disputes and conflicts.[337] Rosenstock concludes that while it may be possible to criticise the [ILC's State Responsibility Articles] for not being more detailed, the Commission has constructed a solid foundation for future development of the law in the light of changing circumstances.[338] Antolin-Jenkins further proposes that the parameters of non-intervention have varied even more over time than have the definitions of use of force, concluding that this very flexibility provides a basis to develop norms specific to cyberspace, without unnecessary encroachment into other areas. She explains: "[b]y the time a treaty defining parameters could be negotiated, it is highly likely that the means of accomplishing tasks defined as cyberwar would have changed". However, as Antolin-Jenkin further observes, doctrines can benefit from negotiation.[339] Also, Grief makes a remark that even with some data processing activities not falling within the scope of the EU law directly, the Member States do not carry "sole responsibility" for national security – although the EU law does not cover national security activities as such, but exercising the "sole responsibility" is not necessarily, or completely, excluded from the application of EU law.[340]

The author developed her approach from the presentation made by Professor Wolff Heintschel von Heinegg at the CCD COE Cyber Conflict Conference in June 2010. In his presentation, Prof. Heintschel von Heinegg suggested that before looking for a new consensus on cyber security issues on international level and before the international community starts processing new legislation, it would be useful to exhaust the solutions, leads and remedies existing under the current legal framework.[341] He proposed a number of "rules" that are based on interpretation of commonly existing legal frameworks. Heinegg's proposals

---

[335] *Supra nota* 213.
[336] See, e.g. Thomas Hoeren, Was ist das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme"? Multimediarecht 2008, Heft 6, p. 365.
[337] *Supra nota* 329.
[338] Robert Rosenstock. The ILC and State Responsibility. 96(4) AJIL 792, 2002.
[339] *Ibid*, p. 17.
[340] *Supra nota* 333.
[341] Wolff Heintschel von Heinegg. CCD COE Cyber Conflict Conference presentation 2010.

were derived from international law of armed conflict, but triggered the author's thinking about how similar discussion starters and conclusions could be derived from other areas of law involved.

Further studies supporting or feeding into the author's approach include those of Sommer[342] and Easterbrook[343], who posit that the legal issues posed by information technology are not novel by definition and therefore can be mitigated by virtue of extension or amalgamation of familiar legal categories.

Also, the findings of Prof. D'Amato on the potential of prohibiting CNA on the basis of customary international law[344], Dr. Vanhamme on the formation and enforcement of customary international law under the practices of the European Union[345], Prof. Rohrmann on the dogmatic function of law as a legal regulation model for cyberspace[346], Prof Hollis on the role of Realpolitik in a current legal interpretation[347] as well as Professors Blume, Reidenberg and Sommer related to the interaction of law and technology have been used to describe the existing *lex lata* and, where applicable, the incentives and rationale for *lex ferenda* in Chapter III.

The author also sees Polanski's conclusions on customary law in the context of the Internet[348] – an attempt to approach legal challenges related to the use of the Internet from a different perspective from that of the body of law governing the use of ICT directly as highly relevant for the further discussion of the approach proposed. In his "Customary Law of the Internet" Polanski suggests that customs of the Internet can be an answer to relevant legal questions given the lack of supranational binding written Internet laws.[349] Polanski has used the theory of international law to explain how the customary behaviour of the Internet society could form the basis of a supranational legal framework for [the commercial sphere of] cyberspace (Internet *lex mercatoria*).[350]

Internet customary practices /…/ are created unconsciously by the community itself and enforced by software, which mechanically imposes certain practices. Internet norms can develop very quickly, within a few years, months or even a couple of hours in case of widespread subscription to automatic

[342] Joseph Sommer. "Against Cyberlaw." – Berkeley Technology Law Journal, Fall 2000.
[343] *Supra nota* 274.
[344] Anthony D'Amato, International Law, Cybernetics, and Cyberspace. – Computer Network Attack and International Law. Michael N. Schmitt & Brian T. O'Donnell eds., 2002.
[345] Jan Vanhamme. Formation and Enforcement of Customary International Law: the European Union's Contribution. – Netherlands Yearbook of International Law (2008), 39, pp. 127-154
[346] Carlos Alberto Rohrmann. The Role of the Dogmatic Function of Law in Cyberspace. – International Journal of Liability and Scientific Enquiry, Vol. 1, No. 1–2 / 2007, pp. 85–93.
[347] Przemyslaw Paul Polanski. Customary Law of the Internet: In Search for a Supranational Cyberspace Law. – TMC Asser Press. The Hague, 2007.
[348] *Ibid*, p. 3.
[349] *Ibid,* p. 2
[350] *Ibid,* p. 4.

update facilities.[351] The idea of custom, Polanski asserts, has advantages. It is a very flexible source of norms, as it reflects changes in the practices of participants and it does so as soon as a change takes place. Its norms are not enacted: they are simply there. It is a source of already enforced norms in a given community, since it reflects what a majority does anyway.[352] From the legal perspective, the concept of custom plays a very important role in interpretation and filling gaps in statutory and conventional laws. [353]

Agreeing with Polanski's approach in principle, the author has omitted the discussion of formation of customary law in the context of the Internet and cyber security from the focus of this dissertation. Since Polanski wrote his book, several major international cyber incidents have occurred and demonstrated how states handle national security relevant cyber incidents. The author has studied these practices to highlight potential disparities between existing and required interpretation of the current legal framework.

This chapter will therefore construct a discussion base for the most frequently referred-to cyber security issues and the legal concepts currently framing those issues. It elaborates existing legal concepts and practices that have proven useful in managing international cyber incidents and, if skilfully combined, linked and developed, could reduce the gray area allowing cyber perpetrators to get away with crime and acts against national cyber security.

3.1. The Principle of Territoriality in Cyberspace

Deriving from Kahn's fourth ground rule [354] that proclaims architectural decentralisation of control at the operations level of the Internet, it is hard to imagine a central body that could govern the Internet by enacting and enforcing laws. Since the early days of the popular Internet, a debate has evolved about the ability to regulate the cyber environment under a territoriality-based legal order. The governance-related freedom of the Internet was advocated by Barlow in the legendary Declaration of Independence of Cyberspace:

> Governments /…/ have no sovereignty [in Cyberspace]. /…/ Cyberspace does not lie within your borders. Do not think that you can build it. /…/ It is an act of nature.[355]

[351] *Ibid*, p. 2.
[352] *Ibid*.
[353] *Ibid.*
[354] Robert Kahn, an American engineer, proposed the TCP/IP in 1974 together with Vinton Cerf. Prior to coming up with the protocol design, Kahn proposed four rules for the architecture of the Internet. The fourth rule proclaims: „There would be no global control at the operations level".
[355] *Supra nota* 76.

Often referred to as the Wild Wild West and the Global Village because of its architecture, the Internet has not been extensively regulated by most governments. This has led to a wide-spread sense of the freedom of the Internet, manifested in anonymity, free speech and freedom of information. Lessig has explained the unrestricted nature of the Internet not as "free" as in "free beer", but "free" as in "free speech", "free markets", "free trade", "free enterprise", "free will" and "free elections".[356] Barlow further contests that governments' concepts of property, expression, identity, movement, and context do not apply to Cyberspace and proposed that due to their inability to understand and control the culture of the Cyberspace, national governments should abstain from imposing regulations on 'global social space'.[357] He suggests that the "online community" form their own Social Contract, and hopefully build a more humane and fair civilisation than governments have made before.[358] As many incidents over the past 15 years have shown, this social contract has not been able to prevent the confrontation between the "inhabitants" of cyberspace and "the real world".

Johnson and Post took the view that geographical borders are meaningless in cyberspace because cyberspace has no borders and boundaries in the traditional sense.[359] At the same time, we can see that neither have the predictions of Lessig[360] on the code-based approach to regulation or Easterbrook's[361] doubts of the existence of cyber law as such come true. Having acknowledged the existence of cyber security related legal challenges several authors have suggested ways to apply existing regulation to cyberspace. There are scholars who argue that the whole conception of the Internet as a place free from regulation should be? repealed and that the Internet could be a place of exquisite control just as it used to be a place of exquisite liberty.[362] Schultz explains that the inherent liberty on the Internet was used as a postulate until it was clearly

[356] Lawrence Lessig. Free Culture (2004) p. xiv. Available at http://www.free-culture.cc/freecontent/ (last accessed May 5, 2011).
[357] *Supra nota* 76.
[358] *Ibid*.
[359] David Johnson and David Post. Law and Borders – the Rise of Law in Cyberspace. 48 Stan. L. Rev. 1367,1370 (1996).
[360] In his „Code is Law", Lessig suggested that the code (i.e. the essence of IT infrastructure) will determine the limits of the permissible in cyberspace and therefore legislative initiatives should be secondary means of shaping behavior of the online community. Lawrence Lessig. Code and Other Laws in Cyberspace. 1999. Available at http://www.code-is-law.org/ (last accessed May 5, 2011).
[361] *Supra nota* 274. Easterbrook asserted that cyber law as such is just a sum of legal provisions existing or to be created under other areas of law and it cannot and should not be regarded as a self-standing legal discipline.
[362] Thomas Schultz. Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface. – The Eeuropean Journal of International Law Volume 19 Number 4, 2008, p. 802.

demonstrated that what we can do on the Internet depends on the laws of technology just as our non-electronic actions depend on the laws of nature.[363]

As Herrera notes, the "placeless-ness" of the Internet is not absolute. He refers to trusted computing and its elements, like certificates, firewalls, digital rights management, static IP addresses etc. that turn segments of the Internet into a tightly controlled and surveilled space by turning every piece of information into a self-surveilling entity.[364]

There are two key arguments regarding the inability of law to deal with the Internet and information technology. One is the aspect of the rapid development of technology that will not be discussed in detail for the purposes of this chapter. The other popular argument for describing regulatory challenges is the cross-border nature of the Internet. Johnson observed in his 1999 conclusions how CNA is different from other means of warfare, and that geography has ceased to be relevant to the security of information systems that are connected to the Internet or that are accessible by radio.[365] The same conclusions were made by Goodman and Brenner in an article dealing with criminal law enforcement issues in cyberspace using the example and case study of the 'Love Bug' virus.[366] Similar observations have been drawn from the analysis of the Law of Armed Conflict – in 1999, Prof. Schmitt concluded that "unless the international community is willing to adopt a de novo scheme for assessing the use of inter-state coercion, any justification, or condemnation of [Computer Network Attacks] must be cast in terms of the use of force paradigm[367], which, as Schmitt observes, is inadequate for safeguarding shared community values threatened by Computer Network Attacks.[368] DeZwart observes that [the Internet] cannot be regulated in the same way as any other form of written or spoken word.[369]

The shift of the cyber security paradigm has resulted in acknowledgment by several governments and international organizations that rules are needed to shape behaviour on the Internet. The question thus becomes how to achieve the regulatory goals. Having studied the evolution of e-commerce regulation and the challenges related to the notions of sovereignty and statehood, Prof. Cox explains that border controls on the Internet are possible to develop and

---

[363] *Ibid*, p. 802.

[364] Geoffrey L. Herrera. Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space.m 1st International CISS/ETH Conference on „The Information Revolution and the Changing Face of International Relations and Security", May 23–25, 2005.

[365] Phillip A Johnson. "Is It Time for a Treaty on Information Warfare?" – International Law Studies, Vol. 76, edited by Michael N. Schmitt and Brian T. O'Donnell, 439-455, p. 441. Newport, RI: Naval War College, 2002.

[366] *Supra nota* 165.

[367] *Supra nota* 26, p. 913.

[368] *Ibid*, p. 886.

[369] Melissa DeZwart. The Future of the Internet: Content Regulation and its Potential Impact on the Shape of Cyberspace. – Entertainment Law Review, Volume 9 Issue 2, February 1998, p. 92.

implement and that many governments have successfully regulated cyberspace. He therefore concludes that nations are increasingly acting in concert to deal with the borderless nature of cyberspace by creating both relatively uniform laws across jurisdictions, and agreements for international cooperation in surveillance and investigation.[370]

So while traditional legal rules on jurisdiction do not fit into the Internet context, the notions of jurisdiction, sovereignty and ownership can used by governments and international organisations to combine international, public and private regulatory efforts. The legal concepts of sovereignty and property allow States to impose necessary obligations to people, processes and policies subject to their jurisdiction. With reference to levels of authority (see Chapter II of this dissertation) there are cyber security related questions that are resolved on the international level (e.g. use of cyber force), on the national level (e.g. limitations to privacy and freedom of expression for national security purposes, sanctions for cyber offenses).

As the Estonian incident's aftermath indicates, several cyber security related regulatory steps need to be taken primarily on the national level even if the need for additional regulation derives from an international, cross-border incident. Only on the national level can decisions be made on what parts of the information infrastructure are critical for the country's functioning, what is the authority of the law enforcement in investigating the incident, what obligations do communication service providers have and what standard of security is required from network operators.[371]

The territoriality principle therefore should be implemented to take as much advantage as possible of the existing jurisdictional structure. The responsibility of a State for securing its own networks can be derived from this rule as due to the legal concepts of non-intervention and sovereignty, only nations themselves can effectively provide for rules and restrictions on security and stability of the information systems supporting their functions and relying on the information infrastructure run in their territory.

According to the UN General Assembly, no State has the right to intervene, directly or indirectly, for any reason whatever, in the internal affairs of any other State.[372] The ICJ has underscored the principle of the non-intervention right of every sovereign State to conduct its affairs without interference.[373] The territorial imperative of public international law derives from the General Assembly's Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States of October 1970: "nothing" in its

[370] Noel Cox. The Regulation of Cyberspace and the Loss of National Sovereignty. Socio-Legal Studies Association, 2002 Annual Conference University of Wales Aberystwyth, United Kingdom 3-5 April 2002.
[371] On the regulatory steps taken in Estonia after 2007 attacks, see *supra nota* 239.
[372] Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty. UNGA Resolution 2131 (1965).
[373] Military and Paramilitary Activities in Nicaragua (Nicaragua vs. United States of America), 1986 ICJ Rep. 14, para 202.

terms shall be construed as authorizing or encouraging any action which would dismember or impair, totally or in part, the territorial integrity or political unity of sovereign and independent States conducting themselves in compliance with the principle of equal rights and self-determination of peoples . . . and thus possessed of a government representing the whole people belonging to the territory without distinction as to race, creed or color.[374,]

The UN Manual for Prevention of Computer-related crime[375] contains a recommendation for states to negotiate agreements on the positive conflicts issue, addressing a) an explicit priority of jurisdictional criteria: for example, of the location of the act over the location of the effect, of the place of physical detainment of the suspect over in absentia proceedings or extradition; b) a mechanism for consultation between the states concerned in order to agree upon either the priority of jurisdiction over the offence or the division of the offence into separate acts, and c) cooperation in the investigation and punishment of international computer offences, including the admissibility of evidence lawfully gathered in other countries, and the recognition of punishment effectively served in other jurisdictions.[376]

In principle, "[a]ny attempt aimed at the partial or total disruption of the national unity and the territorial integrity of a country is incompatible with the purposes and principles of the charter of the united Nations."[377]

While cyberspace as such cannot be subjected to territorial jurisdiction, there is a lot that every government can do to exercise effective control over the IT infrastructure located on its territory – such as providing for a sustainable policy and legal support system? for investments into information architecture and telecommunications market, and developing an understanding of threats and capabilities existing within its jurisdiction to cope with incidents and balance the development of the information society with the interests of national security.

The control over information assets in a State's territory would provide the State and its authorities with effective situational awareness about the nature of the incident as well as the action required to investigate and cooperate beyond the jurisdiction. As Heintschel von Heinegg notes, states should not knowingly allow their critical infrastructures to be used for launching attacks against another state.[378] In case the domestic remedies (e.g. the availability of logs, duty to cooperate by communication service providers, etc.) are not exhausted, it

[374] G.A. Res. 2625, at 121, 124, U.N. GAOR, 25th Sess., Supp. No. 28 (Oct. 24, 1970).
[375] At the 8th Congress on the Prevention of Crime and the treatment of Offenders (held in Havana, Cuba, 27 August – 7 September 1990), the United Nations General Assembly adopted a resolution dealing with computer crime legislation. Based on its Resolution 45/121 (1990).
[376] *Supra nota* 79.
[377] G.A. Res. 1514, at 67, U.N. GAOR, 15th Sess., Supp. No. 16, U.N. Doc. A/4684A (Dec. 14, 1960).
[378] *Supra nota* 341.

would be difficult to justify a request to gather additional information or a request for cooperation from other nations.

Thus, the information infrastructure located within a State's territory is subject to that State's territorial sovereignty. The question then becomes how sovereignty can be exercised under the conditions of "pushed boundaries".

3.2. The Attribution of Cyber Incidents

Attribution has played an important role in recent major international cyber incidents. In 2007, Estonian authorities accused Russia of cyber attacks launched against the Estonian governmental and critical private infrastructure networks.[379] Although the persons responsible for those attacks have never been identified,[380] Russia and hackers operating from Russian territory have been associated with the incident as well as the cyber attacks against Georgia (2008) and Lithuania (2008).

Similarly, China has been accused of launching cyber espionage attempts against US information systems. In early fall 2007, the Chinese People's Liberation Army was reported to have hacked into a Pentagon computer network in the most successful cyber attack on the US DoD to date.[381] Allegedly, it took three weeks and 4 million dollars to "clean up the mess" after the theft of an 'amazing amount of sensitive data' from the Pentagon.[382]

The US is not the only nation having cyber issues with China. Similar messages come from Germany, Belgium and India, all of which claim that computer networks inside their borders are routinely targeted by hackers trying to ferret out information that could benefit the Chinese government.[383] Additional concerns are raised by France, Australia and New Zealand.[384] In 2007, the MI5 alert on a Chinese spy threat was considered UK government-level accusations against China carrying out state-sponsored espionage against British economy.[385]

---

[379] Supra nota 17.

[380] See Eneken Tikk, Kadri Kaska. Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. – ECIW Proceedings 2010.

[381] Sevastopulo, D., McGregor, R., Chinese military hacked into Pentagon. September 3, 2007. Available at http://www.ft.com (last accessed May 5, 2011).

[382] Dan Goodin. Pentagon attackers stole 'amazing amount' of sensitive data. – The Register, March 6, 2008, http://www.theregister.co.uk/2008/03/06/pentagon_breach_assessment (last accessed May 5, 2011).

[383] Dan Goodin. India and Belgium decry Chinese cyber attacks. – The Register, May 8, 2008. http://www.theregister.co.uk/2008/05/08/belgium_india_china_warnings (last accessed May 5, 2011).

[384] Eyden, J. France blames China for hack attacks. – The Register, September 12, 2007. http://www.theregister.co.uk/2007/09/12/french_cyberattacks (last accessed May 5, 2011).

[385] Blakely, R., MI5 alert on China's cyberspace spy threat. – The Times, December 1, 2007. http://www.lexisnexis.com (last accessed May 5, 2011).

The fact of attribution opens the door to finding an entity responsible for the incident.[386] From the state responsibility perspective a state is held responsible when it violates another state's rights, and in doing so proximately causes injury to the latter. Codified in the International Law Commission's Articles on State Responsibility (hereinafter also "the Articles"), the legal foundations of state responsibility define a wrongful act or omission to a state to be when a) attributable to the state under international law; and b) constituting a breach of an international obligation of that state.[387] Under circumstances defined in the Articles and international case law the responsibility is also attributable to persons who are not organs or employees of the state, but act as its agents.[388]

As Brown notes, there are limitations to state responsibility. In case the fact of state control cannot be established, the state cannot be held responsible for action made possible by its breach of international obligations.[389]

Under international law, several threshold markers exist when it comes to state responsibility for malicious cyber activity. According to the MILCW expert group, "if a cyber operation has been launched or otherwise originated from governmental cyber infrastructure there is a rebuttable presumption that the state in question is associated with the operation."[390]

The issue of attribution has also been looked into by international courts. According to ICJ in the Nicaragua Case, "[e]ffective control (financing, organizing, training, supplying and equipping as well as the selection of […] targets and the planning of the whole of its operation is not enough to meet the [attribution] threshold."[391]

According to the Tribunal in the Tadic case, "[o]verall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations is required for meeting the threshold."[392]

Prof. Wolff Heintschel von Heinegg concluded at the CCD COE Cyber Conflict Conference that the fact that an act of cyber attack has been launched from an information and communication system located in a State's territory is

---

[386] On state responsibility, see, e.g. Sir Robert Jennings and Sir Arthur Watts, Eds. Oppenheim's International Law 33 (9th Ed, 1992). See also, Davis Brown. Use of Force against Terrorism after September 11th: State Responsibility, Self-Defense and Other Responses. 11 Cardozo J. Int'e & Comp. L. 1. Spring, 2003.

[387] International Law Commission. Draft articles on Responsibility of States for Internationally Wrongful Acts. Text adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/56/10).

[388] See Article 8 of the Articles.

[389] Davis Brown. Use of Force against Terrorism after September 11th: State Responsibility, Self-Defense and Other Responses. 11 Cardozo J. Int'e & Comp. L. 1. Spring, 2003. Page 863.

[390] Draft Manual for International Law Applicable to Cyber Warfare. Available upon request from the CCD COE Legal and Policy Branch (www.ccdcoe.org).

[391] *Supra nota* 376.

[392] Tadic Case (I.C.T.Y. Case # IT-94–1).

prima facie evidence that the act is attributable to that State.[393] Healey suggests that a more nuanced approach is needed for national responsibility for cyber attacks. He proposes and explains ten categories of state involvement by creating a spectrum of state responsibility.[394] He also notes that due to technical difficulties of identifying the person behind the computer and the denial of nations of being involved in attacks against other nations' critical information infrastructure, the legal standards of Nicaragua[395] and Tadic[396] are beyond reach for the concept proposed.[397]

However, attribution beyond the context of state responsibility can result in different consequences. The other kinds of attribution include identifying the machines, humans or sponsoring organization.[398] Therefore, attribution as an issue is not to be generalised, since different standards for attribution and relevant legal consequences exist –

– to restrict access to communications in case of a malicious activity there is no need to identify the actor – it is sufficient to point out the device;
– to request cooperation from or to impose economic sanctions against a country that lets its cyber infrastructure be used for routing cyber attacks there is no need to attribute the attacks to any specific person – it suffices to define which networks/operators are involved and which jurisdiction they belong to;
– to engage in collective self-defence against a nation state, the decisive factor is the level of hostilities.

Depending on the nature and state of the incident and the kind of attribution available, the remedies available under legal instruments may include assistance from authorities to identify the source of attack, share information about the perpetrators, methods and tools, and ???search, seize and investigate the incident. Also, countries may be expected to raise the level of their cyber security by establishing stronger control over the use and exploitation of the information architecture operated on their territory. Naturally, the balance between the economic and security interests will be established case-by-case basis. We can primarily speak about the? 100% attribution requirement when it comes to law enforcement and prosecution. Here attribution becomes a technical rather than legal issue– the law enforcement usually has the necessary authority to gather evidence about the identity of the perpetrator. If attribution is technically not feasible, the presumption prevails that without sufficient identification the act cannot be attributed to a person.

---

[393] *Ibid.*
[394] Jason Healey. A Vocabulary for National Responsibility for Cyber Attacks. Presentation at the CCD COE Cyber Conflict Conference. Tallinn, 2010.
[395] *Supra nota* 374.
[396] Tadic Case (I.C.T.Y. Case # IT-94–1).
[397] *Supra nota* 397.
[398] ARDA, BAA 03-03-FH, „Information Assurance for the US Intelligence Community, 2003. Available at http://www.slideshare.net/butest/ardainsiderbaa030-3858786, last accessed June 25, 2011.

It seems to be generally accepted that the fact that a cyber attack has been launched from an information system located in a State's territory invokes the responsibility of that State for the attack. The attribution rule however is likely to become the most controversial and disputed one.

3.3. Cooperation to Counter Cyber Attacks

The Internet and information infrastructure by their essence and structure combine the public and private sector, thus making it almost impossible for the state to effectively protect information infrastructure without the private sector's cooperation.[399] With the vast majority of the world's information infrastructure being privately operated and owned, remedies to cyber conflict need to be developed in public-private partnership.

Although the private sector is generally responsible for securing their systems, cyber war could change the types of attacks faced by companies.[400] In the Estonian case the political tension between the Estonian and Russian authorities resulted in denial-of-service attacks against communication service providers, online media and the banks. As recognised later on a regulatory level, pieces of private information services and equipment have become part of national critical infrastructure.[401] Under the contemporary cyber conflict paradigm, the private sector can therefore fall under attack because of the actions undergone by the government.

Besides public and private sector interdependence, cooperation is necessary between nations due to the cross-border nature of cyber conflict these days. In the Estonian case in 2007 cooperation was rendered by dozens of countries to analyse, mitigate and investigate cyber attacks. The cross-border nature of the Internet and incidents requires cooperation between nations.

Different legal constructs exist for cross-border and public-private cooperation. For example, the E-Commerce Directive requires Member States to cooperate with other Member States by appointing contact points for exchanging information.[402]

Under Article 23 of the Cyber Crime Convention, the Parties are requested to co-operate with each other through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the

[399] *Supra nota* 6.
[400] See, e.g., Unsecured Economies: Protecting Vital Information. – McAfee, January 21, 2009, http://www.mca-fee.com/us/about/press/corporate/2009/20090129_063500_j.html (last accessed May 5, 2011).
[401] *Supra nota* 239.
[402] Article 19 (2) of Directive 2000/31/EC (*supra nota* 51).

collection of evidence in electronic form of a criminal offence.[403] There are several other instruments of the Council of Europe addressing the issue of cross-border legal/judicial cooperation in criminal matters[404]. The most relevant in the context of pre-trial investigation of cybercrime is the European Convention on Mutual Assistance in Criminal Matters with its additional protocols.[405]

Article 4 of the North Atlantic Treaty requests the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.[406] This provision will be used for coordinating the Allies' responses to cyber attacks short of "cyber armed attack".

The requests for cooperation can also be based on bilateral agreements. The Estonian request for assistance to the Russian Federation in 2007[407] was based on the Mutual Legal Assistance Agreement[408].

Although in need of specification on the national level as to points of contact and more detailed list of activities, these provisions form a wide-ranging legal framework for cooperation between interested parties for the purposes of enhancing cyber security.

Cooperation has *de facto* also occurred without with? less defined legal bases – the activities of national CERTs (CERT stands for Computer Emergency Response Team) involve constant consulting and information exchange as well as sharing expertise and practices to detect, analyse and mitigate malicious activities targeting national or critical private information systems and services. It is only recently that nations have started looking into detailed regulation of CERTs' activities.

Another practical example of *ad hoc* cooperation is the take-over of the hosting of Georgia's governmental websites during the Russo-Georgian War and the accompanying cyber attacks in 2008 by several governments.

Cooperation therefore is both a widely recognised legal concept and the practical behavioural pattern arising from the fact that under the current cyber conflict paradigm and interconnectedness of the information infrastructure it would be impossible for any nation to defend itself against cyber attacks

---

[403] *Supra nota* 49.

[404] See the list of treaties: conventions.coe.int/Treaty/Commun/ListeTraites.asp?MA=20&CM=7&CL=ENG, 11 April 2008. (last accessed June 25, 2011).

[405] *European Convention on Mutual Assistance in Criminal Matters*, signed on 20 April 1959, Strasbourg. Available at conventions.coe.int/Treaty/en/Treaties/Html/030.htm; *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, signed on 17 March 1978, Strasbourg, available at conventions.coe.int/Treaty/EN/ Treaties/HTML/099.htm; *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, signed on 8 November 2001, Strasbourg. Available at conventions.coe.int/Treaty/EN/Treaties/HTML/182.htm. (last accessed June 25, 2011).

[406] *Supra nota* 132, Article 4.

[407] See more *supra nota* 383.

[408] Agreement on Mutual Legal Assistance and Legal Relations in Civil, Family and Criminal Matters, signed on 26 January 1993. RT (State Gazette) II 1993, 16, 27; RT II 2002, 14, 58.

without the cooperation of those States through whose infrastructure the attacks are routed or those authorities that have effective visibility on the activities. Even 'local' crimes may have an international dimension, and assistance may be required from all countries through which an attack was routed. An example is the case of 'Mafiaboy', whose distributed denial of service attacks in February 2000 was a watershed event: the seriousness of the threat and the vulnerability of e-commerce became apparent.[409]

Because of the nature of information infrastructure and the cost of cyber security, cyber incident handling requires cooperation between national authorities. Effective coordination of capabilities and efforts would allow authorities to better exploit benefits of different technical, legal and policy solutions across the whole spectrum of cyber security. For example, the implementation of Personal Data Protection[410] and Data Retention[411] Directives in a coordinated manner for cyber security concerns of national authorities would result in availability of traffic data to all potentially interested parties as well as a more holistic approach to data protection.

Furthermore, cross-disciplinary cooperation is also necessary between experts of legal, policy, military, technical and other areas of expertise to skilfully combine the methods and solutions of each area into an effective "cyber shield".

Cooperation may take various forms. Consulting, information exchange, reallocation of resources or supporting services under attack all can be considered potential ways to implement this rule. The international legal framework for cooperation needs to be supported by national provisions for Internet service provider cooperation, data exchange and partnerships as well as international coalition agreements.

From international cooperation perspective, the fact that a cyber operation has been conducted via the cyber infrastructure located in a state creates a duty to cooperate with the victim state.

3.4. Self-Defence Against Cyber Attacks

In the context of emerging cyber security challenges and nation-states engaging in cyber warfare capability development, the ramifications of self-defence have become an important deterrence factor.

A distinction needs to be made between two types of self defence: self-defence in the context of the laws of war, and self-defence in the context of criminal law.

---

[409] *Supra nota* 165, p. 418.

[410] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

[411] *Supra nota* 86.

The right to self-defence in response to cyber incidents under the law of armed conflict needs to be assessed in the light of the broader concept of the use of cyber force extensively discussed in legal theory before and after the rise of cyberspace.[412] As elaborated by Prof. Schmitt more than a decade ago, unless the international community is willing to adopt a *de novo* scheme for assessing the use of inter-state coercion, any justification or condemnation of computer network attacks must be cast in terms of the use of force.[413] With reference to the Nicaragua case, Schmitt concludes that the use of force line must lie somewhere between economic coercion and the use of armed force.[414] Schmitt further offers criteria for delimiting economic and political coercion from the use of armed force and accentuates that it is not any use of force, but an "armed attack" which gives a state the right to respond in self-defence.[415] For a Computer Network Attack to rise to the level of armed force it must cause results identical to those of kinetic warfare, specifically direct human injury or physical damage to tangible property.[416]

Schmitt's analysis focuses on the criteria under *the jus ad bellum*, to computer network attack.[417] After 10 years, the international community has accepted the premises provided by Schmitt and today the "Schmitt Test" is a

[412] See, e.g. Ian Brownlie. International Law and the Use of Force by States (1963); Yoram Dinstein. War, Aggression and Self-Defence. Cambridge University Press, 4th Edition, 2005. Also, Marco Benatar. The Use of Cyber Force: Need for Legal justification? In Goettingen Journal of International Law I, 2009, Vol. 3, pp. 375–396.

[413] S*upra nota* 26, p. 913.

[414] *Ibid*, p. 914.

[415] *Ibid*, p. 920.

[416] *Ibid*, p. 922.

[417] *Ibid,* p. 886. Schmitt proposes criteria to delimit economic and political coercion from the use of armed force. These criteria include: 1) *severity*: armed attacks threaten with physical injury or destruction to property to a much greater degree than other forms of coercion. Physical well-being, security of body and of property occupy the foundation of the human hierarchy of need. 2) *Immediacy* – the negative consequences of armed coercion, or threat of those consequences, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodation is hampered in the former case. 3) *Directness* – the consequences of armed coercion are more directly tied to the *actus reus* than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition of use of force precludes negative consequences with greater certainty. 4) *Invasiveness* – in armed coercion, the act causing the harm usually crosses the border into the target state, whereas in the use of economic warfare, the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the sovereignty of the target state and, therefore, is more likely to disrupt international stability. 5) *Measurability* – while the consequences of armed coercion are usually easy to ascertain (e.g. a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force. 6) *Presumptive legitimacy* – in most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exemption such as self-defense. 7)

valuable tool for military commanders and their advisers for assessing the level of hostilities.[418] Schmitt also concludes, however, that in the absence of any significant practice there is no basis in the state practice to extend the concept of force to cyber operations and consequently there is not sufficient ground for developing a customary norm.[419]

"Armed attack" is a variation of the use of force that justifies the use of force in self-defence as an exception to generally established prohibition of any use of force under Article 2(4)[420] of the UN Charter. The legal criteria for invoking individual and collective self-defence are established under customary law as well as provided for in the UN charter and international case law. According to Article 51[421] of the UN Charter, states have the inherent right of individual or collective self-defence if an armed attack occurs against a UN Member State. In sum, a cyber attack only invokes individual and collective self-defence if it rises to the threshold of an "armed attack".

The assessment of whether a cyber attack by its effect, consequences or nature is equivalent to an armed attack will be made by national authorities, and in case of a request for collective action, also by international partners (e.g. by the North Atlantic Council in case article 5 of the North Atlantic Treaty[422] is invoked). Recently, policy statements have been made by several nations about their potential military responses to cyber attacks. These statements contain unfortunately little specific criteria for such a judgment.

Political statements often also lack clear distinction between use of force and armed attack and therefore provide no additional clarity to the current doctrine. The US stated in a recently published strategy document that it reserves the right to use all necessary means – diplomatic, informational, military and economic – to defend the nation and its allies, partners and interests, seeking broad international support whenever possible.[423] As stated by the Estonian Minister of Defence a few days later: "If cyber attacks create substantial economic damage, disruption of the functioning of the society and human losses it should be handled as a matter of national security and we should react

[418] *Supra nota* 257.
[419] *Supra nota* 26, p. 921.
[420] Article 2(4) of the UN Charter: All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.
[421] Article 51 of the UN Charter: Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.
[422] *Supra nota* 139, Article 5.
[423] Cheryl Pellerin. White House Launches US International Cyber Strategy. American Forces Press Service, May 17, 2011.

accordingly. We should determine our response to an attack based on the damage it causes or was intended to cause, not the type of weapon employed. Depending on the nature and scale of the attack, the response to it would include a wide range of possible options, including military."[424]

In the absence of legal practice the concept of "cyber self-defence" can primarily be seen as a theoretical deterrent against most severe forms of cyber threats. However, considering recent debates relating to NATO's Cyber Defence Policy review and national statements on military reactions to cyber attacks, the topic remains one of the most disputed in the current cyber security paradigm.

Collective self-defence is considered to be NATO's core commitment. The NATO 2020 Expert Group concludes, however, that the requirements for fulfilling that commitment have shifted in shape.[425] There are increasingly less doubts about whether an unconventional danger – such as a cyber attack – triggers the collective defence mechanisms of Article 5 provided it rises to the level of severity of an armed attack.[426]

In the event Article 5 is invoked by one or more of the Allies, this will have to be determined by the North Atlantic Council based on the nature, source, scope, and other aspects of the particular security challenge. For the purposes of planning, NATO should assume that serious threats will in fact materialize; preparations for detection, deterrence and response should be calibrated accordingly. These preparations, which should encompass adequate military capabilities, appropriate training exercises, information gathering, and strategic assessments, must correspond to the full range of potential Article 5 threats.[427]

It is therefore crucial to develop a better understanding of what constitutes a "potential Article 5 threat". As suggested by authors, the criteria could involve the level of hostilities, the targets[428] (e.g. critical national infrastructure, systems critical to a state's vital interests) or the motivation[429] (hostile intent). The qualitative criteria for classifying CNA not only according to the consequences, but the "consequence affinity with the current prescriptive distinguishers"[430] were developed in the early days of cyber warfare doctrine development to address the need to respond to computer network attacks *comparable to* armed attacks "until the international community casts off its current cognitive approach". [431]

---

[424] Comments made by Defence Minister Mr Mart Laar on the issue regarding cyber and physical attacks, Tallinn, une 1, 2011.
[425] *Supra nota* 146, page 8.
[426] *Supra nota* 415 (Benatar), page 393.
[427] Ibid, page 20.
[428] See, e.g. Benatar (*supra nota* 415); Walter G. Sharp. Cyberspace and the Use of Force. 1999, p. 129. Eric Talbot Jensen. National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Stanford Journal of International Law. Summer 2002, p. 224.
[429] *Supra nota* 431 (Sharp), p. 131.
[430] *Ibid*.
[431] *Ibid*.

Another long-disputed aspect of self-defence is whether it is a responsive or preventive legal concept. As Murphy explains, self-defence refers to the use of armed coercion by a state against another state in response to a prior use of armed coercion by the other state or by a non-state actor operating from that other state.[432] Anticipatory self-defence, in turn, refers to the use of armed coercion by a state to halt an imminent act of armed coercion by another state (or by a non-state actor operating from that other state).[433]

From a criminal law point of view, acting in self-defence excludes liability for an otherwise wrong act. In other words, criminal law allows for the use of defence anytime the victim reasonably believes that unlawful action is or is about to be used against him. This is not to claim that every 'hack-back' can be justified under the concept of self-defence[434] – this legal concept is usually seen as a last resort for the attacked.

According to Article 31 (c) of the Statute of the International Criminal Court, criminal responsibility is excluded if the person acts reasonably to defend himself or herself or another person or, in the case of war crimes, property which is essential for the survival of the person or another person or property which is essential for accomplishing a military mission, against an imminent and unlawful use of force in a manner proportionate to the degree of danger to the person or the other person or property protected.

So far, no cyber attack has risen to the threshold of self-defence and consequently, no military response has been given to a cyber attack to date. From a legal point of view a kinetic response in self-defence against a cyber attack can be permissible provided that it is necessary to achieve the aim of the act (e.g. putting an end to the attack) and that the counter-attack is proportionate considering the method and effect of the aggression.

As no cyber incident has so far triggered action in self-defence, there seems to be certain natural deterrence in the concept of applicability of the Law of Armed Conflict to cyber incidents of sufficient intensity. While the decision about what would constitute a cyber armed attack needs to undergo technical, legal and policy debate, the practical aspect of self-defence is to further develop the understanding what remedies are available in case this threshold is crossed.

The baseline for self-defence therefore potentially entitles both individuals and nation states, and can be targeted against nations and non-state actors. The conditions and limitations to exercising this right require either additional state practice or more detailed threat assessments from the international legal point of view. Unlike in cases of kinetic attacks, the time and jurisdiction factors are more problematic to take into account.

A distinction also needs to be made between prevention measures, counter-measures and self-defence. When it comes to criminal law, it is necessary to

[432] Sean D. Murphy. The Doctrine of Preemptive Self-Defense. Villanova law Review, Volume 50, 2005, p. 703.
[433] *Ibid*.
[434] *Supra nota* 242.

consider technologically feasible scenarios of self-defence as well as the national case law in the field. Without realistic understanding about which cyber intrusions can be effectively defended against at what stage of their preparation or occurrence it will be difficult for the lawyers to judge the legality of such action taken. As Jayawal, Yourcik and Doss explain, the timing of the decision to hack back is crucial along? with the mobility of the attacker and the economic losses mounting.[435] It would, however, be difficult to justify traceback as a means of self-defence provided the attack is already affecting the system. At the same time, without effective source tracing, no effective countermeasures such as containment, redirection, or back-hacking can be implemented.[436] Similarly, it would be difficult to see installation of anti-hack" products and the use of honeypots[437] as remedies of self-defence. For these considerations, the limitations of self-defence under criminal law need to be analyzed and clarified in conjunction with data protection law and certain aspects of criminal proceedings.

For the purposes of further discussion, it can be taken as a point of departure that everyone has the right to self-defence when facing a clear and imminent danger. The conditions and limitations to exercising this right derive from public international law as well as criminal law.

3.5. Data Exchange and Personal Data Protection

With cyber incidents being cross-border by nature and the architecture of the Internet not allowing centralised control over online activities, information exchange about threat patterns, anomalies in network traffic and on-going incidents is crucial for determining the appropriate and applicable measures for defence and security. The industry of deep packet inspection, intrusion detection, etc., is based on the idea of monitoring and analysing network traffic. As Altford emphasises, the only reasonable measure of effectiveness is detecting cyber infiltration when it happens.[438] Altford further notes that, when discovered, an incident needs to be reported to other entities including not only those responsible for mitigation, but also potential victims.[439]

The balance between network monitoring and information exchange needs to be carefully assessed against individuals' right to privacy.[440] Although there are

---

[435] *Ibid*.
[436] *Ibid*.
[437] A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. (http://searchsecurity.techtarget.com/definition/honey-pot).
[438] Lionel Altford, Cyber Warfare: Protecting Military Systems. – Acquisition Review Quarterly, Spring 2000, p. 116.
[439] *Ibid*.
[440] See, e.g. Lee A. Bygrave. Data Protection Law: Approaching Its Rationale, Logic and Limits. Kluwe Law International, 2002.

examples of the balance between citizen-government privacy shifting (e.g. after the 9/11 attacks in the United States)[441], Westin foresees building stronger privacy controls into emerging technologies to make sure that these are held to high accuracy requirements and used in a proper way, along with developing online privacy-enhancing technologies that are both effective and user-friendly.[442] Blume, in contrast, observes that data protection rules restrict information technology and that data protection must be balanced and must respect the fact that there are societal reasons for the application of technological developments.[443]

Despite diverging scholarly opinions, data exchange regulation is relatively well established from the legal perspective, especially in the EU countries. Directive 95/46/EC[444] (Data Protection Directive) serves as the basis for personal data protection legal acts in nearly 30 advanced information societies. Currently, personal data can flow between the 27 EU member states and three EEA member countries (Norway, Liechtenstein and Iceland) and to Switzerland, Canada, Argentina, Guernsey, and the Isle of Man. An exception is granted to the US Department of Commerce under the Safe Harbour Privacy Principles, and for the transfer of Air Passenger Name Records to the United States Bureau of Customs and Border Protection. Further regulation on traffic data is provided in the e-Privacy Directive.[445]

According to the EU Data Protection Directive, any information relating to an identified or identifiable natural person is regarded as personal data.[446] EU data protection supervisory authorities also regard IP addresses and other network monitoring and incident handling data as personal and thus subject to processing restrictions arising from the EU Data Protection Directive.[447] Such restrictions include the requirement of the data subject's consent for processing

---

[441] See, e.g. Daniel L. Solove. "I've Got Nothing to Hide", and Other Misunderstandings of Privacy. 90 CAL. L. REV. 2002, pp. 1095–99.

[442] Alan F. Westin. Social and Political Dimensions of Privacy. Journal of Social Issues, Vol. 59, No. 2, 2003, p. 450.

[443] Blume (*supra nota* 7), page 18.

[444] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, available at http://eurlex.europa. eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. (last accessed June 25, 2011).

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

[446] Article 2.

[447] See Aoife White, IP Addresses Are Personal Data, E.U. Regulator Says January 22, 2008, available at http:// www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html. (last accessed June 25, 2011). Also, Bygrave (*supra nota* 443) page 317.

data[448], the prohibition to transfer data to third countries[449] as well as potential inadmissibility as evidence of such data as it has been obtained in an unlawful manner.

Currently, a considerable divide exists between the legal and technical approaches to data and its security. What makes the data protection regulation controversial in practice is the lack of adherence to it by information technology experts because of differing understanding of network monitoring economics from legal and technical perspectives. In short, one possible interpretation of the Directive leads to the conclusion that collecting and exchanging IP-addresses is subject to the terms and conditions provided for in the Directive.[450] The other leaves IP addresses out of the immediate scope of applicability and only requires the Directive to be followed in case the use of IP addresses actually will be used to identify the person behind it.

While there are counter-arguments to regarding IP addresses *per se* as personal data also from the legal perspective[451] , it is important to note that at the current time this perception can only be changed and mitigated on the national level. The Data Protection Directive shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.[452] A similar construct is provided in the Council of Europe's Data Protection Convention. This instrument allows derogation from the basic principles of data protection when such derogation constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences.[453]

To sum up, a more detailed and nuanced approach is needed for categorizing data as personal and deciding whether or not it attracts the status of protection under Data Protection regulation when it comes to processing personal data for

[448] Pursuant to Article 7 of the Data Protection Directive (supra nota 362) theMember States shall provide that personal data may be processed only if:the data subject has unambiguously given his consent.

[449] Pursuant to Article 26 (1) of the Data Protection Directive (supra nota 362) the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

[450] In more detail, Eneken Tikk. IP Addresses Subject to Personal Data Regulation. – International Cyber Security Legal and Policy Proceedings. CCD COE Publications 2010, p.s 24-40.

[451] Ibid. Also Blume, *supra nota* 7.

[452] Article 3 (2) of the Data Protection Directive.

[453] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.1981. Article 9 (2).

cyber security purposes. To detail the events of processing where data is not regarded as personal within the meaning of the Directive, it is essential to keep in mind the spectrum of cyber security and, where necessary, use the possible exception to the applicability of the Directive.
As long as national approaches mature, information infrastructure monitoring data is perceived to be personal and therefore subject to personal data protection regulation unless provided for otherwise.

3.6. Access to Information and Early Warning

As discussed under the data exchange section, when a cyber attack occurs, the detecting entity should immediately inform all possible targets. The principle, whereby an irrevocable threat needs to be reported to potential victims, also called "early warning", has always been regarded a technicality rather than legal concept. It is well established as best practice between "operational" cyber security entities such as CERTs. From the legal perspective, the right of the public and the potential victim or affected party to be informed about the threat is supported by the principle of access to information and the obligations of the communication service providers.

Under Article 10 of the European Convention of Human Rights[454] a general right exists to receive and impart information. On the national level the access to information right has been developed into a more specific right to be informed about threats and risks. For example, the Estonian Public Information Act requires that public authorities disclose promptly any information concerning danger which threatens the life, health or property of persons or the environment, select the quickest and most suitable manner of averting danger and alleviate the possible consequences.[455]

According to Article 4(2) of the Directive on Privacy and Electronic Communications[456], in case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk, and where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

The concept of early warning has also been supported by recent cyber incident handling practices. In 2008, 300 Lithuanian websites were defaced in response to the Parliament's decision to ban the use of soviet symbols. According to the Lithuanian CERT the majority of the attacked Web sites were hosted on a single web server. Lithuanian government agencies were warned of

[454] The European Convention on Human Rights, Rome 4 November 1950.
[455] § 30 (1) of the Public Information Act. Available at http://www.legaltext.ee/et/andmebaas/tekst.asp-?loc=text&dok=X40095K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=avaliku+teabe.
[456] *Supra nota* 448.

an impending Web attack, and therefore mounted appropriate defences and were able to cope with the attacks when they started on June 28, 2008.[457]

The fact that Lithuanian governmental agencies were informed of the attacks beforehand raises the issue of the standard of service level agreements (SLAs) for governmental information infrastructure, as well as considerations for the necessity of defining a non-discrimination duty to ensure that both public and private sector ISP-s and web hosts are warned about known threats. Increasingly, governments make available and the public uses a variety of governmental services online; the Lithuanian eGovernment services with their high record of use of are an excellent example here. All these services are provided under SLAs with mainly private-sector ISPs. Governments in countries with a high degree of cyber threat need to consider additional guarantees for their services and information infrastructure and a way to achieve this would be to apply for a higher level of services in terms of sustainability of electronic services, availability priorities, and reaction time.[458]

As early warning practices, if supported by legal constructs, provide transparency about the threats and attacks, considerable counter-arguments exist to disclosing information about threats, targets and remedies. The private sector is increasingly becoming a target of the politically motivated attacks and therefore also subject to the overall threat picture. It may not be in the business interests of the banks and telecommunication service providers to disclose information about their vulnerabilities and damages. Also, disclosure of particular information may affect the rights of their clients. The balance between access to information and early warning requirement therefore needs to be balanced against the interests of business confidentiality and secrecy.

For the purposes of further discussion on the limitations and conditions of the early warning concept under law, the general principle supported under international law is that the public has the right to be informed about threats to their life, security and property. As in the case of privacy, possible limitations to this right include national security.

3.7. Duty of Care of Cyber Security Stakeholders

As discussed in Chapters I and II, cyber security is a collective effort where the role of stakeholders (international organizations, governments, private entities and individuals) are not always predefined. Therefore, it is essential that every stakeholder acknowledges and implements due care when engaging in its respective role.

An obligation to patch software is not necessarily directly established under law. Imposing clear and ultimate obligations on service providers is not a common practice in all countries. Although principles exist that require service

[457] Rainys, Rytis. RRT. In an e-mail (10 Dec 2008) to the CCD COE Legal Team.
[458] *Supra nota* 17.

providers to implement „adequate measures“ to secure their networks, it is often disputable what is the „due diligence“ and a “reasonable user” or a “reasonable communications service provider” standard in cyber security.

Neglect derives from the legal duty to act. It is therefore important to look into the duties related to electronic communications, cyber crime and, potentially, cyber warfare.

Under the EU Directive 95/45/EC[459] pertaining to processing personal[460] data, Member States are obliged to provide that personal data must be processed fairly and lawfully (Article 6 (1) a)) and that the controller[461] must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing (Article 17 (1)). In other words, everyone in control of processing personal data is responsible for its confidentiality, integrity and availability in accordance with the its original purpose. Regarding the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. A similar requirement is imposed by the Directive on Privacy and Electronic Communications – the service providers are expected to take appropriate technical and organisational measures to safeguard security of its services.[462]

Under the Directive 2000/31/EC[463], the standard for hosting provider’s liability is provided. In case of actual knowledge of illegal activity and awareness of facts and circumstances from which the illegal activity or information is apparent, the information service provider is obliged to act to remove or to disable access to such information (Article 14 (1)).

The Council of Europe’s Cyber Crime Convention[464] sets an international standard for cyber crime obliging Parties to adopt such legislative and other measures as may be necessary to establish as criminal offences under domestic

[459] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031 – 0050. Available online at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[460] Article 2 (a) defines as personal data and therefore potentially is applicable to processing of “any information relating to an identified or identifiable natural person ('data subject')”. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

[461] Article 2 (d) defines controller as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

[462] *Supra nota* 448, Article 4 (1)

[463] *Supra nota* 51.

[464] *Supra nota* 49.

law, when committed intentionally, the access to the whole or any part of a computer system without right (Article 2).

The duty of care standard in humanitarian law [465] has been recently developed in relation to collateral damage analysis has recently beenthis sentence – needs to be split up? Don't understand it associated with military reconnaissance and precision strike capabilities, considered "to good to permit good-faith mistakes", thus suggesting that the American military cannot afford using its advanced capabilities negligently. [466] Rudesill observes that under LOAC's duty of care, as in negligence law under tort and agency, responsibility for effects generally varies with control and the four core principles of LOAC (military necessity, discrimination, proportionality and humanity) form the base of this duty.

Reaching through the whole spectrum of cyber security, the duty of care standard, if applied consistently by all stakeholders, can significantly reduce vulnerabilities. All stakeholders of cyber security have a duty to care in adhering to the laws of electronic communications, crime and war, and a negligence standard (although not yet fully developed in all areas) is appropriate where intent to violate law cannot be established.

As cyber threats of political context become more prevalent, the duty of care concept can be used to develop and impose security standards for critical information infrastructure and governmental or military information services. It will be up to each entity to assess its risks not only from a business perspective but also considering its posture in national critical infrastructure list and applicable sectorial/national threat assessments. The measures for defence and mitigation need to correspond to the general threat assessment and be developed in cooperation with respective supervisory authorities.

An example is the Emergency Act[467] adopted in Estonia after the lessons learned from 2007 attacks. It requires the provider of life-critical services to implement the necessary level of security in information systems and information assets supporting life critical services (§ 40). While the providers are given the freedom to choose the means of providing the adequate level of security, they are responsible for the end result.

The court concluded that when a new technology has been shown to be so extensive as to be a nearly universal practice or custom, there was a duty on the part of the tug owner to supply effective receiving sets. It further stated that

[465] See, e.g. Michael N. Schmitt. Bellum Americanum: The US View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict. 19 Mich. J. Int'l L. 1081, 1998.

[466] Dakota S. Rudesill. Precision War and Responsibility: Transformational Military Technology and the Duty of Care Under the Laws of War. The Yale Journal of International Law. Summer 2007, Volume 32, No.2, p. 518.

[467] RT I 2009, 39, 262.

„there are precautions so imperative that even their universal disregard will not excuse their omission.“[468]

Every individual, company and State has the responsibility to implement a reasonable level of security in their information and communication assets and activities.

3.8. Criminalisation of Cyber Offenses

It is well established in law that individuals can only be prosecuted under criminal law for the acts defined as crimes. The need for improved quality of criminal law for the purposes of better securing the information society has been advocated by many for a variety of reasons.[469]

It is practically impossible to impose State coercion on any individual engaged in a cyber attack unless the specific activity and/or consequence have been listed as a crime under national law. Broadhurst notes that the need for reliable and efficient mechanisms for international cooperation in law enforcement matters has never been more urgent and cites Esposito[470] on that the fight against cyber-crime either is a global one or it makes no sense.[471]

In 1996, the European Committee of Crime Problems concluded that given the cross-border nature of information networks, a concerted international effort was needed to deal with [misusing facilities of the cyber-space]. Only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena.[472] In the framework of such an instrument, in addition to measures of international co-operation, questions of substantive and procedural law, as well as matters that are closely connected with the use of information technology, should be addressed.[473]

The first round of cyber criminalisation was passed a decade ago when the United States in launched the Cyber Crime Convention[474] initiative. The aim of

---

[468] The T. J. Hooper; The Northern No. 30 and NO. 17; The Montrose; Petition of Eastern Transport. CO.; New England Coal & Coke CO. v. Northern Barge Corporation; Hartwell & Son, Inc., v. Same 53 F.2d 107; 1931 US Dist. LEXIS 1744 (U. S. District Court, S.D. N. Y., 1931); The T. J. Hooper; The Northern No. 30 and NO. 17; The Montrose; Petition of Eastern Transport. CO.; New England Coal & Coke CO. v. Northern Barge Corporation; Hartwell & Son, Inc., v. Same 60 F.2nd 737 (U. S. Ct. App., 2nd Circuit, 1932). Cert. denied 287 US 662; 53 S. Ct. 220; 77 L. Ed. 571; 1932 US LEXIS 387 (1932).

[469] For a technical perpective, e.g. Richard Clayton. Complexities in Criminalizing Denial of Service Attacks. Available at http://www.cl.cam.ac.uk/~rnc1/complexity.pdf (last accessed June 25, 2011). For a sector-specific approach, e.g. Pauline Reich. Cybercrime, Cybersecurity, and Financial Institutions Worldwide. In: Cyberlaw for Global E-business: Finance, Payments and Dispute Resolution (2008).

[470] G. Esposito. The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument?— Broadhurst, R. Ed, Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong. 2004.

[471] *Supra nota* 223, p. 415.

[472] *Supra nota 222,* para 9.

[473] *Ibid.*

[474] *Supra nota* 49.

the Convention adopted in 2001 and in force since 2004 is to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data. The Convention criminalises the following conduct: illegal access and interception, data and system interference, misuse of devices, computer-related fraud and forgery and offences related to child pornography and copyright and related rights.[475]

Thus, a general agreement these days exists on the need to reinforce criminal law to adapt to the developing cyber criminality trends. To date, 30 nations have done it using the model of the Council of Europe Convention.[476]

The implementation of the Convention to contemporary cyber threats is challenging in that depending on national criminal policy different restrictions may apply to the scope of an offence. The Convention on Cybercrime provides various legal solutions for illegal access (Article 2) and illegal interception (Article 3) only. Some countries have decided to extend the protection that is available through technical measures by criminalizing data espionage. Some countries follow a narrow approach and criminalise data espionage, only where specific secret information is obtained – an example is 18 USC. § 1831, that criminalises economic espionage. This provision not only covers data espionage, but other ways of obtaining secret information as well.

The various approaches to the criminalisation of illegal computer access at the national level show that enacted provisions sometimes confuse illegal access with subsequent offences, or seek to limit the criminalisation of the illegal access to serious violations only. Article 2 ("Illegal Access")[477] of the Cybercrime Convention has been implemented by Austria, Czech Republic, France and Slovak Republic, whereby in Austria[478], access to the whole or any part of a computer system without right is restricted with the following criteria:

---

[475] See more *supra nota* 71.

[476] *Supra nota* 49, aiming to facilitate international cooperation, detection, investigation and prosecution of cyber crime and calls for establishing a common basis for substantive and procedural law and for jurisdiction, is open for signature by the member states and the non-member states which have participated in its elaboration and for accession by other non-member states. Currently the total number of signatures not followed by ratifications is 18; the total number of ratifications/accessions is 28 (Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine and as a non-member the United States). Available:
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

[477] *Supra nota* 49, Article 2: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

[478] Strafgesetzbuch – StGB, BGBl 1974/60.

intention to obtain computer data, economic gain for the perpetrator or disadvantage for another person and violation of safety precautions.[479] In the Czech Republic, the aggravating circumstances are set as a prerequisite of higher punishment: the punishment is higher if the offence results in substantial damage or if the offender acquires a substantial benefit. Article 323–1 of the French Penal Code[480] criminalises fraudulent accessing or remaining within all or part of an automated data processing system without any restrictive criteria. The Slovak Republic's Criminal Code[481] regards as an offence the obtaining of unauthorised access to a computer system or another information carrier or to a part of it with the intent to cause a damage or any other prejudice to another, or to obtain undue advantage for himself or for another and to make unauthorised use of the information contained there. The offence must be committed with dishonest intent.

The development of a comprehensive legal framework addressing the challenges of cyber crime therefore comprises national approaches but rests on regional and international approaches. Besides the Cyber Crime Convention and relevant activities by the Council of Europe, the European Union, G8, OECD and INTERPOL have started to work towards a more comprehensive cyber crime regulation and have engaged in the fight against cyber crime.[482] Their instruments, though not all legally binding, provide valuable insights into designing national approaches that best support national cyber security interests and avoid gaps and inconsistencies pointed out by existing national practices. The need for wider harmonization of national and regional approaches has been pointed out by numerous scholars.[483]

Schjolberg has highlighted the need to revise the Cyber Crime Convention from the perspective of emerging trends and threats. However, for many

---

[479] Section 118a of the Austrian Penal Code. Analysis based on: Markko Künnapu. Council of Europe Convention on Cybercrime. European Union Framework Decision on Attacks Against Information Systems: Comparative Study on the Implementation and Recent Developments. 2008, p. 7-8. CCD COE Publishing, 2008.

[480] http://195.83.177.9/upl/pdf/code_33.pdf (last accessed May 5, 2011).

[481] Act No. 140/1961 of the Collection of Laws.

[482] For different international approaches and isntruments, see *supra nota* 71; Also Warren B.Chik. Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore. (2007). Research Collection School of Law. Paper 348. Available at http://ink.library.smu.edu.sg/sol_research/348 (last accessed June 25, 2011). Roderic Broadhurst. Developments in the Global Law Enforcement of Cyber Crime. – International Journal of Police Strategies and Management. Vol. 29, Issue. 3.

[483] See Xingan Li. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Available at http://www.webology.ir/2007/v4n3/a45.html (last accessed May 5, 2011). Abraham D. Sofaer, Seymour E. Goodman. Cyber Crime and Security. The Transnational Dimension. Hoover Institution Press, 2001. Stein Schjolberg. The History of Global Harmonization on Cybercrime Legislation – the Road to Geneva. December 2008. Available at http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (last accessed June 25, 2011).

countries, politically motivated cyber attacks have not existed in the list of national cyber threats and so no substantial legal policy has advanced in this respect.

In principle all necessary investigatory techniques and measures for fighting cyber crime are covered by instruments such as the Cyber Crime Convention[484] and national procedural laws. What needs to be fine-tuned is criminal policy in the field. Broadhurst explains by referring to Newman and Clarke how crime prevention occurs in the e-commerce context. In the online 'situation' the theft of information and the manipulation of identity and trust are the key. In their approach, crime is an opportunity that occurs when the following conditions combine in time and place: the presence of motivated and tempted offenders (offender pathology is not required), and attractive and tempting targets in the absence of effective guardians. When this situation arises crime will occur providing the offenders also have appropriate resources (i.e. social and technical capital) to undertake the crime.[485]

To sum up, while the Cyber Crime Convention provides the vehicle for combating cyber crime of differing scope and scale, it contains restrictions and standards that need to be tuned in to national legislation to achieve the necessary settings for investigation and prosecution. With cyber crime developing political dimensions, the consensus on the remedies needs to be widened to achieve more comprehensive deterrence. The obligation to criminalize most common cyber offenses under national law therefore comprises both substantive and procedural criminal law as well as national review of instruments for international cooperation.

3.9. Clarity of Mandate and Authority

The need for a clear mandate for stakeholders in exercising their roles and responsibilities as part of the comprehensive cyber security picture derives from the interrelation of nations and public-private partnerships, different national approaches and sometimes overlapping, sometimes conflicting expert and entity views. Whenever a cross-border coordinated effort into the underlying values of the cyber security is required, international organisations play an important role in concerting these efforts. The issue of defining and coordinating international efforts of global cyber security gains practical importance especially from the perspective of developing or revising existing cyber security agendas (and potentially, relevant instruments) on national and international levels.

To justify governmental "investments" in their cyber capabilities, international organisations need to make better use of and enhance efforts undertaken by their counterparts. While, for example, NATO's primary focus in the field could be related to collective self-defence procedures, the organisation still

[484] *Supra nota* 100.
[485] *Supra nota* 223, p. 416

needs an agenda for handling cyber incidents below the threshold of a "cyber armed attack", targeted both against the organisation itself and the individual Allies.[486] Prior to deciding which measures need to be put in place between the Allies for defending against an incident, it is necessary to understand the already existing legal framework, capabilities and trends in order to avoid conflicting practices and gaps in coordination. As emphasised by the Group of Experts in the NATO 2020 Report –

> For all its assets, NATO is by no means the sole answer to every problem affecting international security. NATO is a regional, not a global organisation; its authority and resources are limited and it has no desire to take on missions that other institutions and countries can handle successfully.[487] /…/ NATO is strong and versatile but it is by no means well-suited to every task. Other organisations, national governments and nongovernmental entities can lead the way toward such vital goals as economic reconstruction, political reconciliation, improved governance, and the strengthening of civil society. Depending on the needs in any particular case, NATO may serve as the principal organiser of a collaborative effort, or as a source of specialised assistance, or in some other complementary role.[488]

Currently the mandates of international organisations are loosely defined when it comes to cyber security. Weak coordination of their agendas on both national and international levels results in gaps and overlaps of focus areas. For instance, international cyber crime related harmonisation has been focused on by at least seven major international organisations. Li observes that cyber crime is tackled by several organisations which can be categorised as professional, regional, multi-national or global.[489] For states party to a number of international organisations, the question becomes, what is the input of every organisation to the national cyber security framework? Currently, the on-going activities in the Council of Europe, the European Union, the United Nations and other organisations in the field of cyber crime are transparent only to those closely engaged in the field.

Of course, there are unique characteristics to each organisation's activities, such as membership, specific issues under attention, legal status of the instruments, etc. This all needs to be taken into account when making decisions on the national level related to supported initiatives and developments.

---

[486] See also *supra nota* 133.
[487] *Supra nota* 146, p. 9.
[488] *Ibid*, p. 10.
[489] *Supra nota* 486 (Xingan Li).

3.10. The Rules of Behaviour for International Cyber Security

For a way forward, compiling a list of cyber security legal issues alone would not suffice. Yet the first methodological step of developing the concept was to examine the 'issue lists' of legal scholars with different area of expertise. With hundreds of scientific articles written on legal issues of cyber security, the approach of systemizing or even listing issues beyond one area of law will narrow down the scope and focus of further discussion.

Inspired by Prof. Heintschel von Heinegg and having in mind the goals acknowledged by the international organisations, the author has designed this chapter to reflect proposed rules after discussing briefly the legal issues and relevant provisions of international instruments.

The issues raised in Chapter III relate to different legal areas. While some (e.g. data exchange, cooperation of ISPs) are primarily subject to regulation under telecommunications law, some (criminalisation, self-defence, criminal cooperation) relate to criminal law and process and others (state responsibility, self-defence in case of an armed attack) belong to the regulatory area of primarily international law and the Law of Armed Conflict. A few legal concepts (duty of care, mandate) are broad enough to reach through several legal areas. Therefore, a comprehensive legal discussion to balance the views and goals of related legal areas (law pertaining to information society, telecommunications, cyber crime, national security and cyber warfare) is required for determining critical gaps, conflicting provisions and necessary exceptions.

Overall, there is no consensus between nations on what, if any, additional regulation is needed on the international level to better secure the cyber domain. Instead, several nations have expressed the view that it is first necessary to "test" the limits of existing legal instruments and frameworks to understand the existing "rules of behaviour" and only then proceed to deciding where law needs to be amended and how.

The author therefore proposes a set of "rules" to promote interdisciplinary legal discussion on where the limits of existing legal frameworks are when it comes to interpretation and implementation of the legal concepts elaborated on in this chapter. The author, by proposing this set of legal statements, hopes to promote focused debate on the quality of existing legal frameworks regarding territoriality, responsibility, cooperation, duty of care, data exchange, access to information, criminalisation, authority and mandate.

This approach does not offer new regulatory approaches, but is intended to invoke constructive discussion about the commonly accepted rules of behaviour for the purposes of cyber security. Essentially, the author takes the view, based on the analysis of existing views and approaches, that it is not possible to offer conclusive legal solutions to cyber security as defined for this thesis, from one legal area perspective only.

Each proposed rule has exceptions and counterarguments to it. Further research and analysis on these is expected to contribute to discussion of commonly agreed base rules as well as explanatory remarks regarding their scope of applicability, exceptions and implementation practices. Therefore the proposed statements are expected to be altered, developed and extended in later discussions.

The author hopes that focusing legal research on these statements instead of problem areas or questions could take a step closer to developing a consensus or clearer schools among experts and therefore contribute to international legal developments discussions in the longer run.

Customary practices of Internet users could be used by governments to harmonise relevant national legislation. Adoption of such norms in national legislations would not only help to standardise, modernise and interpret Internet-related laws in various jurisdictions but would also give them more credibility, because new laws would reflect what the majority does anyway. In this way, a legislator could lessen or even avoid a serious issue of enforcement of Internet-related laws.[490] The same approach could be taken by international, intergovernmental and regional organisations interested in the development of international Internet law.

As discussed in Chapter III, the discussion starters for the Rules of Behaviour are as follows:

The Territoriality Rule: The information infrastructure located within a State's territory is subject to that State's territorial sovereignty.

The Attribution Rule: The fact that a cyber attack has been launched from an information system located in a State's territory invokes the responsibility of that State for the attack.

The Cooperation Rule: The fact that a cyber operation has been conducted via the cyber infrastructure located in a State creates a duty to cooperate with the Victim State.

The Self-Defense Rule: Everyone has the right to self-defense when facing a clear and imminent danger.

The Data Exchange Rule: Information infrastructure monitoring data is perceived personal unless provided for otherwise.

The Access to Information Rule: The public has the right to be informed about threats to their life, security and property.

The Early Warning Rule: Everyone has to notify the potential victims about an upcoming cyber attack.

The Duty of Care Rule: Everyone has the responsibility to implement a reasonable level of security in their information infrastructure.

The Criminalisation Rule: Every nation has the obligation to render possible the investigation of cyber crime and the prosecution of cyber criminals.

The Mandate Rule: An entity's capacity to act (and regulate) derives from its mandate.

---

[490] *Supra nota* 347, p. 3.

SUMMARY

These days, no state is safe from cyber attacks. Since the large-scale cyber attacks on Estonia's government, telecommunications infrastructure, banks and online media in 2007, the global perception of cyber threats has drastically changed. Politically and ideologically motivated cyber attacks on critical infrastructure have been a wake-up call for security experts and have revealed differing views and interpretations among legal communities.

Before the Estonian incident, organisations tended to treat their risks and arrangements in isolation. Cyber security was merely the sum of individual contingency plans having little to do with more systemic risks. What coordination of defences existed involved developing uniform and standard solutions rather than plans or capabilities for coordinated action. Since 2007, however, the United Nations, NATO, the European Union, OSCE and other international organisations have introduced new cyber-security policies or revised existing ones. The concept of cyber incident has been expanded, reaching from internal security breaches to computer crime against critical information infrastructure as well as cyber warfare.

Cyber incidents of the past three years indicate that the reliance on information infrastructure and service has developed to a point where it is becoming possible to undermine the functionality of governments and support political objectives of nations. The mandate of computer security has grown in complexity and seriousness as information technologies have saturated society and, simultaneously, the threats have multiplied in number and sophistication. The term "cyber security" links computer security to notions of national security and is typically articulated by government authorities, corporate heads, and leaders of other non-governmental sectors.

From regulatory and legal analysis perspective, the picture is becoming more and more complicated. First, cyber security itself is getting more and more complex and complicated – major cyber incidents have proven that cybercrime has not fallen back and is more sophisticated and dangerous than ever. Apparently, the legal framework built in the last decade to tackle cyber crime has not proved efficient in the context of national security-relevant cyber incidents like Estonia (2007), Georgia (2008), Conficker (2009), Stuxnet (2010) and many more. Cyber attacks often touch upon the threshold of national security and potentially may reach to the threshold of an armed attack. From the discussions about the adequacy of the current legal and policy framework to respond to contemporary types of cyber attacks and recent revisions of national strategic responses to cyber incidents that the world has recently witnessed, it becomes evident that the cyber security environment is changing and requires additional attention from the national security perspective.

For many nations that are part of the information society, cyber threat perceptions have emerged from a "foreign" context where the US represents the most exploited target for different incidents as well as – from a national security

and military perspective. For the US this has been a natural approach and status considering that the Internet was born in the US military laboratories in 1960s. The EU countries have traditionally devised cyber security strategies focused on extending and strengthening the internal market. Thus, their legal and regulatory focus has been less balanced against national security and military involvement in cyber security. Recently, a group of nations has developed that have "hands-on" experience with cyber attacks and can therefore share their experience. However, lessons learned by Estonia and Georgia remain distant for nations not sharing similar vulnerabilities and political context. Deriving from these lessons learned, cyber security will need to be based on technological developments and the underlying architecture of the information society, correspond to current national and international policy concerns and ultimately, materialise in a regulatory framework supporting the former two.

International discussions have led to more determined steps towards re-shaping the national cyber security strategies and filling the gaps in laws that have allowed politically motivated cyber attacks to remain non-punishable. As the technology develops and the society adopts it, the challenges for regulation change – as do priorities for legal policy and legal interpretation.

The author observes in the first chapter of this dissertation how the change in technology and information society has defined new cyber security challenges. She elaborates on the definition and scope of "cyber security" as understood in the EU and the United States. She looks into how cyber security has become an important agenda item for international organizations and concludes that there is a wide consensus on international level between political and expert groups on the need to develop a comprehensive approach to cyber security.

Based on international calls for a comprehensive approach to cyber security, the author summarises that such an approach will cover the information society development aspect, tackle cyber crime, strengthen national security and be responsive to a wide variety of risks and threats, including politico-military dangers. The author therefore concludes that a comprehensive defence in the cyber context requires getting rid of a stove-piped approach to cyber security planning and encourages synergy between information society design, criminal policy planning, law enforcement capabilities and military defence. A comprehensive approach also requires a combination and coordination of tools, methods and approaches to enhance the global cyber security environment. An ideal solution would serve and balance the purposes and concerns of technology, policy and law.

The author then proceeds to offering a corresponding regulatory framework in Chapter II. She concludes that instead of a specific threat, cyber threats should be regarded as a spectrum where different stages and effects of cyber incidents are aligned. Depending on the motivation, effects and actors, a cyber incident will be categorized as breach of internal regulations, breach of law short of cyber crime, crime, national security relevant incident or cyber warfare. The spectrum of cyber conflict is covered by several legal areas (information society/telecommunications law, criminal law, national security law and law of

armed conflict). The author concludes that the spectrum of cyber conflict ranges from breaches of internal policy or regulations (not patching software, for example) to breaches of legal obligations (such as not reporting illegal activity) to crime to national security threats to outright cyber warfare ('cyber armed attack'). The levels and sources of law relating to cyber security range from the soft (standards and best practices) to organisational (contracts and internal regulations) to national to international agreements and customary law, which inform the four key legal areas the law of network and information security (also referred to as cyber law or information-society law), dealing with, for example, data protection, e-commerce, electronic communications and access to information; criminal law (offences, investigation, cooperation); national-security law and possible restrictions to human rights and liberties resulting from national-security concerns; and the Law of Armed Conflict.

With different areas of law involved in cyber security, the legal concepts involved in cyber incident handling need to be developed, applied and interpreted in a coherent manned to achieve efficient coordination between legal areas. Concepts such as e-commerce, IT procurements, freedom of expression, privacy and others are so far primarily regarded as belonging to the area of the regulation (and implementation) of information society law or cyber law. Cyber crime law combines elements of computer crime and relevant procedural aspects whereas the Law of Armed Conflict is intended to define the threshold and framework of military responses to cyber incidents. From a regulatory perspective, it is essential to look at these legal areas in a systematic and coherent way to identify related concepts and possible areas of confusion.

The author also observes that law is but one aspect and tool for cyber incident handling. In the context of a comprehensive approach law becomes just one area of expertise and one set of instruments to be applied in order to achieve wide-base coordination and mitigation of cyber security.

The author concludes that given the divided and diffuse focus of international organisations, the primary responsibility for addressing cyber security threats and responses currently lies with national governments. Without a thorough understanding of threats and remedies available on the national level any debate on the international level would lack focus. Only after interdisciplinary expert discussions and clarification of national views can the areas for common concern be referred to in detail sufficient for constructively debating additional legal remedies needed.

While the names and distinct lines of authority differ by country, the trend moves towards a cross-governmental approach to national cyber security that would define and cover the whole spectrum of information society development, exploitation and defence issues. This way, legal measures designed to create a more competitive and convenient information society for users would be balanced and combined with national cyber threat assessment concerns as well as planned in a manner satisfying the potential needs of law enforcement, intelligence and military. International organisations' approaches potentially shape and influence national development and implementation of cyber security

strategies and regulations and accordingly, what needs to be implemented by nations depending on their membership in particular organisations.

Based on these observations, having regard to the nature and current setup of the information society and in conjunction with the study of recent national strategic approaches to cyber security, the structure of cyber security legal and policy measures comprises different stakeholders, levels of intervention, methods of prevention, detection and response, as well as hierarchies of decision-making and guidance. A comprehensive structural approach to cyber security therefore needs to consider all relevant legal areas, levels of regulation and concepts. Chapter II focuses on developing and explaining the regulatory framework for a comprehensive approach to cyber security.

As the nature of the conflict changes, so must the law. Contemporary cyber threats can only be confronted by combining the regulation, remedies and legal practice of these four key areas of law. With cyber security reaching through different areas of law, it has only recently become seen as an interdisciplinary problem in law. Interdisciplinary approaches in law are not exceptional but there rarely exist phenomena that cover so many distinct areas of law with equal intensity.

In Chapter III, the author has taken an interdisciplinary analytical approach to existing legal frameworks and with reference to the analysis of existing international legal instruments and recent state practice in resolving cyber incidents, concluded that there is no immediate need to apply law by analogy to cyberspace activities as this would, under diverse opinions and interpretations, not increase certainty and uniformity among states, courts and international organizations about international law. Chapter III focuses on the existing regulations that are designed with different elements of cyber security in mind or reflect generally accepted legal principles that can be applied to cyber space. Taking a closer look at already existing international legal and policy frameworks, the author concludes that most legal constructs we need to tackle cyber security issues exist under international law, although scattered around different instruments of different scope and often in need of cross-disciplinary interpretation according to the contemporary threat context.

There are indications of the need for revision of current interpretation and implementation practices in virtually all legal areas dealing with cyber security. However, the nature of cyber conflict, national priorities and expert opinions are still evolving. Chapter III therefore constructs a discussion base for the most frequently referred-to cyber security issues and the legal concepts currently framing those issues. It elaborates existing legal concepts and practices that have proven useful in managing international cyber incidents and, if skilfully combined, linked and developed, could reduce the gray area allowing cyber perpetrators to get away with crime and acts against national cyber security.

The author proposes an instrumental legal framework for cyber security by discussing cyber security related legal issues and key findings that can lead to further discussion about the area of applicability and limitations of existing legal instruments. In this dissertation, draft rules focused on these issues and

working solutions arising from discussions among experts or in the course of cyber-incident handling are identified after discussion of current legal approaches to key cyber security issues. The rules offer an abstract but concentrated view of the legal topics affecting the handling of cyber incidents and cyber security in general, and highlight the disparity between legal theory and practice. They are intended to focus international debate on the quality and interpretation of existing law rather than the need for new legal frameworks. Several issues sometimes considered as legal, such as attribution, identification or criminal cooperation are, as a matter of fact, related to political or technical aspects and need to be considered from the perspective of constructive solutions. Issues seen as challenges for new legislation, for example data protection or Internet service-provider (ISP) liability, can, moreover, be solved through interpretation of or simple exceptions from existing legal constructs instead of a wholly new legal approach.

This dissertation concludes that cyber activities are also, directly or indirectly, subject to a number of legal instruments which need to be reinforced in consideration of the contemporary cyber threat picture. It is aimed at breaking the myth of legal frameworks (or actually, the lack of regulatory responses) being the key shortcoming on the way to effective cyber security. Various legal constructs exist that, if interpreted and implemented with recent incidents and practices in mind, could foster and support global and national efforts to counter cyber threats.

The concepts discussed in Chapter III relate to different legal areas. While some (e.g. data exchange, cooperation of ISPs) are primarily subject to regulation under telecommunications law, some (criminalisation, self-defence, criminal cooperation) relate to criminal law and process and others (state responsibility, self-defence in case of an armed attack) belong to the regulatory area of primarily international law and the Law of Armed Conflict. A few legal concepts (duty of care, mandate) are broad enough to reach through several legal areas. Law in the cyber security context is not a science in itself – it develops on the basis of emerging social constructs (such as, for example, the interconnectedness of networks and the needs for international coordination resulting thereof) and has regard to the requirements of the society, including, in the given context, the measures and methods required to mitigate cyber incidents. Before deciding what legal measures are needed on international level, it is necessary to combine and exhaust the already existing legal concepts.

The author concludes that for a way forward, compiling a list of cyber security legal issues alone would not suffice. Inspired by Prof. Heintschel von Heinegg and having in mind the goals acknowledged by the international organisations, the author has designed this chapter to propose a set of potential cyber security rules of behaviour after discussing briefly the legal issues and relevant provisions of international instruments.

The concept of the Rules is focused on the quality of existing legal framework regarding territoriality, responsibility, cooperation, duty of care, data exchange, access to information, criminality and mandate. It does not offer new

regulatory approaches, but is intended to invoke constructive discussion about the commonly accepted rules of behaviour for the purposes of cyber security. Naturally, each rule has exceptions and counterarguments to it. The discussion is expected to contribute to discussion of commonly agreed base rules as well as explanatory remarks regarding their scope of applicability, exceptions and implementation practices. Therefore the proposed statements are expected to be altered, developed and extended in later discussions.

The author takes the opinion that discussing the rules could take us a step closer to developing a consensus or clear schools among experts and therefore contribute to international discussions in the longer run.

SUMMARY IN ESTONIAN

Doktoriväitekirja "Laiapõhjalise küberjulgeoleku õiguslik raamistik" kokkuvõte eesti keeles

Küberjulgeoleku mõiste ja olemus on viimaste aastatega oluliselt muutunud. Infoühiskond on arenenud faasi, milles riik ja ühiskond tervikuna on muutunud infotehnoloogiliselt haavatavaks. Ühtlasi on ootuspäraselt sagenenud riikliku tähtsusega infosüsteemide ja elutähtsate infoühiskonna teenuste vastu sunatud poliitilise konteksti ja motivatsiooniga ründed. Seega ei piirdu küberohud enam üksnes arvutikuritegevusega vaid hõlmavad ka ohte riigi julgeolekule ning võivad riikide sõjaliste võimete arendamise tulemusena eskaleeruda sõjapidamiseks küberruumis.

Uutele ohtudele ja haavatavustele on aastaid tähelepanu juhtinud ka Arquilla, Aldrich, Denning ja paljud teised peamiselt Ameerika Ühendriikide arvutiturbe- ja julgeolekueksperdid. Rahvusvahelise ulatusega arvutiturbeintsidendid Eestis (2007), Gruusias ja Leedus (2008) ja strateegiliste võrkude ja objektide vastu suunatud pahavara (Conficker, 2009; Stuxnet, 2010), aga ka sõna- ja infovabaduse ning riikliku julgeoleku tasakaalu testiv Wikileaks (2010), sagenevad katsed selgitada arvutivõrkudesse tungimise teel välja riikide sõjalisi võimeid (GhostNet) ning ühiskonna ja riigi toimimiseks oluliste teenuste (valimised, juurdepääs avalikule teabele) vastu suunatud ründed (Birma 2008, 2010; Iraan 2009, Raadio Vaba Euroopa, 2007) on aga alates 2007. aastast hoidnud „küberjulgeoleku" küsimused rahvusvaheliste organisatsioonide ja foorumite päevakorras. Ehkki arvuti- ja võrguturbe temaatika on paljudes riikides ka varem aktuaalne olnud, keskendus küberjulgeolek näiteks Euroopa Liidu riikides seni eeskätt infoühiskonna kaitsele ja arvutikuritegevuse vastu võitlemisele.

Infotehnoloogia ja poliitika eesmärkide ja meetmete segunemine nõuab rahvusvaheliste seisukohtade, aga ka praktiliste õiguslike lahenduste väljatöötamisel suurt pingutust, kuna arvutiturbe ja riikliku julgeoleku valdkondades nähakse infoühiskonna arendamisel erinevaid probleeme ning sellest tulenevalt jõuavad erinevad eksperdid erinevate metoodiliste lähenemistega erinevate seisukohtade ja tulemusteni.

Jurisdiktsioonide ja erialaekspertide käsitluste ja mõistekasutuse lahknemisest tulenevalt erinevad põhimõtteliselt infotehnoloogiaekspertide ja julgeolekuasjatundjate hinnangud sellele, kas Eestit 2007.a. tabanud teenustõkestusrünnete näol oli tegemist ohuga riiklikule julgeolekule või mitte. Infotehnoloogiliselt on teenustõkestusründe näol tegemist võrdlemisi lihtsa ning levinud ründevõttega, mille toimepanemine on jõukohane eriliste ressursside ja koordineerimiseta. Seetõttu järeldavad infoturbeeksperdid, et Eesti valitsuse väited, nagu oleks neid 2007. aasta aprillis ja mais tabanud enneolematu ulatusega ründed ei ole arvuti- ja võrguturbe seisukohalt põhjendatud. Seevastu poliitilisel tasandil on Eesti sündmused viinud rahvusvahelise julgeoleku tagamisele keskenduva Põhja-Atlandi Lepingu Organisatsiooni küberkaitse poliitika ja kontseptsiooni väljatöötamiseni. Seda põhjusel, et tehniliselt lihtsate rünnete

tulemusena tekkis sündmuste ahel, mis ohustas riigi toimimist, ühiskonna eluviisi ning tekitas ulatusliku majandusliku kahju. Lisaks on Eestit 2007.a. tabanud teenusetõkestusründe id meedias nimetatud Esimeseks Kübersõjaks ning toodud sageli näiteks kübersõjaks valmistumise vajalikkuse põhjendamisel.

Autor asub seisukohale, et kuni erialaekspertide ning poliitikute vahel valitseb eriarusaam sündmuse olemuse ja mõju teemal, on ühtsete tegevusplaanide ja meetmete väljatöötamine, aga ka ühtse õiguspraktika kujunemine raskendatud. Valdkonnapõhine riskide hindamine viib killustatud arusaamani ühiskonnas infotehnoloogia toel toimivate suhete ja protsesside mõjudest ja turvalisusest. Nende tähelepanekute pinnalt on rahvusvaheline üldsus viimaste aastate jooksul jõudnud järeldusele, et arvutiturve ja riiklik julgeolek moodustavad ühisosana uue ainevaldkonna („küberjulgeolek"), mille tagamiseks on vajalik laiapõhjaline koostöö ning koordineerimine.

Küberjulgeoleku (*cyber security*) mõistet kasutatakse täna peamiselt kahes tähenduses. Esiteks kasutatakse seda üldise terminina, millega mõistetakse küberruumi osade kaitset kõikvõimalike rünnete eest (näiteks asutuse süsteemide kaitse – küberturve/küberturvalisus). Teiseks kasutatakse terminit rahvusvahelises kontekstis, kus ta räägib küberturvalisusest/ küberjulgeolekust kui uuest julgeolekuohust (nt Eesti Küberjulgeoleku strateegia on tõlkes *Cyber Security Strategy*). Sagedasem kasutamise kontekst on hiljuti lisandunud riigi ja rahvusvahelise tasandi julgeolekudimensiooni, mis on tekkinud seoses riikide ja ühiskondade üha suuremast sõltuvusest ja seotusest infotehnoloogiliste vahendite ja lahendustega. Seejuures räägitakse küberjulgeolekust peamiselt kahes veidi erinevas kontekstis – riiklik küberjulgeolek (st küberohud, mis on ohtlikud konkreetse riigi suunal, vrd USA-s on nt arvutispionaaž Eestist oluliselt aktuaalsem teema) ja rahvusvaheline küberjulgeolek, mis keskendub eeskätt nendele küberohtudele, mida ei saa pidada ühe või väikese grupi riikide probleemiks (nt *non-state actors*).

Selgitamaks antud väitekirja aluseks olevat probleemi ning väitekirja põhiteesi, on esmalt vajalik anda ülevaade kaasaegse küberjulgeolekuolukorra kujunemisest ja põhisuundadest. Autor on väitekisra esimeses peatükis käsitlenud Interneti ja infoühiskonna arengut, vaadelnud viimaste aastate jooksul sagenenud poliitilise motivatsiooniga arvutiturbeintsidentide konteksti ja mõjusid, samuti erinevate riikide ja rahvusvaheliste organisatsioonide seisukohavõtte seoses küberjulgeoleku tõhustamisega ning järeldanud, et seni paralleelselt eksisteerinud kontseptsioonide (arvutiturve ja riiklik julgeolek) sisu ja ulatus on infotehnoloogia kiire arengu ja laialdase kasutuselevõtu tõttu muutumas või isegi segunemas. Sellest tulenevalt on vaja kombineerida kahe valdkonna (infotehnoloogia ja julgeolek) põhimõtted ja mõistebaas ning saadud tulemused infoühiskonna edasise kujundamise ja reguleerimise aluseks võtta. Sellest, kuivõrd edukad on eksperdid antud ülesande täitmisel, sõltub edasine infoühiskonna arengu poliitika kujundamine, õigusloome ning tehnilised normid ja standardid, aga ka julgeoleku tagamise eest vastutavate ametkondade loend ning nende täpsemad õigused ning kohustused.

Töö seisukohalt on termini „küberulgeolek“ ning sellest lähtuvate mõistete (küberrünne, küberohud jt) sisu ja ulatus olulised, kuivõrd töö keskmes olev „laiapõhjaline õiguslik lähenemine“ (*comprehensive legal approach*) küberjulgeolekule keskendub sellest lähtuvatele elementidele ja probleemidele nende kogumis, toetades erinevate organisatsioonide, erialavaldkondade, avaliku ja erasektori ühtlustatud lähenemist küberjulgeoleku problemaatikale õiguslikust perspektiivist. Nagu autor esimeses peatükis järeldab, on küberjulgeoleku täpne sisu ja ulatus, seega ka laiapõhjalise lähenemise täpsem sisu täna alles tuvastamisel. Kõige üldisemalt peaks see hõlmama poliitilisi, tsiviil- ja sõjalisi vahendeid ja meetmeid arvutivõrkude ja infoühiskonna turvalisuse tagamiseks. Seetõttu annab autor töö esimeses osas laiapõhjalist küberjulgeolekut käsitlevate või toetavate organisatsioonide ja autorite põhjal ülevaate antud lähenemise põhielementidest. Nende põhjal esitab autor omapoolse nägemuse küberjulgeolekuohtudest, nende õiguslikust olemusest ja konkreetsetele ohu tüüpidele kohalduvatest õigusvaldkondadest ja -intituutidest.

Alates 2007.a. on mitmed riigid ja rahvusvahelised organisatsioonid oma küberjulgeoleku alaseid strateegia- ja poliitikadokumente läbi vaadanud ja uuendanud eesmärgiga kaasata küberjulgeoleku tagamisse lisaks õiguskaitseorganitele ka julgeolekuasutused, kaitsejõud, aga ka majandus- ja poliitikaeksperdid. Kui mõnedes riikides nõuab küberjulgeoleku kaasajastamine senisest tõhusamat koordineerimist küberjulgeoleku erinevate aspektide eest vastutavate valitsusalade ja asutuste vahel, siis paljudes maades tuleb küberjulgeoleku alane võimekus alles välja kujundada. Autor järeldab viitega erinevate riikide ja rahvusvaheliste organisatsioonide tööle küberjulgeolekuohtude ja nende ennetamiseks ja tõrjumiseks vajalike meetmete kaardistamisel, et seoses küberjulgeoleku kontseptsiooni laienemisega ning laiapõhjalise lähenemisega küberjulgeolekule on vajalik luua või ühendada asjakohased õiguslikud meetmed ja vahendid. Laiapõhjalist küberjulgeolekut toetav õigusloome ja -praktika peab lähtuma küberjulgeoleku uuenenud kontseptsioonist.

Esimeses peatükis esitatud ülevaatest nähtub, et traditsiooniline probleemipõhine lähenemine arvutiturbeintsidentide õiguslikule reguleerimisele ja analüüsile ei toeta laiapõhjalist küberjulgeolekut, kuivõrd iga intsidenti ja probleemi vaadeldakse üksnes konkreetsest ekspertvaldkonnast lähtuvalt ega hinnata selle võimalikku eskaleerumist ega mõju küberjulgeolekule tervikuna. Lähtudes üldiselt omaksvõetud vajadusest koondada küberjulgeoleku tagamisse nii rahu- kui sõjaaegsed meetmed ja vahendid, rahvusvahelisel tasandil püstitatud eesmärgist saavutada laiapõhjaline kaitse kaasaegsete küberohtude vastu ning paljude riikide poolt küberjulgeoleku ühe keskse probleemina väljatoodud kehtiva õiguse ebapiisavuse väitest esitatakse käesolevas doktoritöös kaks keskset hüpoteesi.

Esmalt püstitab autor hüpoteesi, et kaasaegse küberjulgeoleku õigusliku raamistiku kvaliteedi hindamine ei ole võimalik ühe õigusvaldkonna piires. Küberjulgeoleku õiguslik raamistik moodustub infoühiskonna ja elektroonilise side õiguse, kriminaalõiguse, riikliku julgeoleku õigusliku raamistiku ning

rahvusvahelise sõjaõiguse pinnalt ning nõuab eelnimetatud valdkondade seoselist käsitlust.

Antud väite tõestamiseks selgitab autor esmalt küberjulgeolekuohtude ulatust ning erinevat tüüpi ohutude õiguslikku kvalifikatsiooni. Nii konstrueerib autor esmalt esimese peatüki pinnalt küberjulgeoleku regulatiivse ja rakendusliku raamistiku, skaleerides kaasaegsed küberohud ning selgitades nende kaetus erinevate õigusvaldkondadega. Seejärel kaardistab autor nendesse valdkondadesse kuuluvad olulisemad õigusinstituudid eesmärgiga selgitada seoseid õigusvaldkondade ja instituutide vahel ning näidata, et küberjulgeoleku-intsidendi tüübist või ka staadiumist olenevalt kohaldub sellele erinev õigusvaldkond, mis aga laiapõhjalise küberjulgeoleku eesmärke arvestades nõuab seoselist lähenemist kõnealuste õigusvaldkondade arendamisele ja rakendamisele. Teisest peatükist nähtub, et õiguse rakendamine küberjulgeoleku valdkonnas on seotud diplomaatia, korrakaitse, sõjanduse, luure, majanduse ja poliitika meetmete ning tegevustega, mistõttu tuleb õiguse rakendamisel arvestada nende valdkondade toimimisprintsiipe ja praktikat. Autor seostab omavahel olulisemad küberjulgeoleku tagamisega tegelevad valdkonnad, millest autori hinnangul lähtub nii õiguse tõlgendamiseks vajalik mõiste- ja teadmiste baas kui ka sisend õigusloomesse. Edasi vaatleb autor küberjulgeoleku institutsionaalset raamistikku, mille kaudu selgub normide hierarhia ning nende andmiseks ja rakendamiseks pädevad ametkonnad, aga ka normide adressaatide ring. Autor selgitab, et küberjulgeoleku tagamisse on erinevas pädevuses ning ulatuses vajalik kaasata nii rahvusvahelised organisatsioonid, riigivõim, erasektor kui ka kodanikud. Eraldi toob autor välja rahvusvaheliste organisatsioonide tänase tegevuse küberjulgeoleku tagamisel ning selgitab seoseid riikliku ja rahvusvahelise küberjulgeoleku meetmete ja vahendite vahel.

Teiseks asub autor seisukohale, et sageli küberjulgeoleku ühe keskse probleemina esile toodud õigusliku raamistiku puudumine on üksnes näiline, kuivõrd alles kujuneva laiapõhjalise lähenemise juures on interdistsiplinaarsed õiguslikud vaated ja tõlgendus alles kujunemas ning kitsalt spetsialiseerunud õiguseksperdid lähtuvad analüüsil ja tõlgendamisel eeskätt "oma" valdkonnast. Tuginedes teises peatükis esitatud tähelepanekutele õigusvaldkondade seoselise käsitluse vajadusele, arvukale erialakirjandusele ja eksperthinnangutele, toob autor välja küberjulgeoleku tagamisega seotud õigusprobleemid, mis vajaksid küberjulgeoleku tõhustamiseks laiemat analüüsi ning tähelepanu. Autor soovib juhtida tähelepanu vajadusele arvestada õiguse edasisel arendamisel, aga ka rakendamisel uuenenud ohuolukorda ehk eluliste asjaolude ulatuslikku muutumist, mis omakorda tingib vajaduse mõista õigust ning määratleda normide kohaldatavus uues sotsiaalses tegelikkuses. Teame, et seaduse teksti tähenduse mõistmisel on abiks erialadefinitsioonid, mis aga küberjulgeoleku puhul on kasutusel ebajärjepidevalt või alles kujunemisjärgus. Näiteks infotehnoloogiaga seotud õiguse tekste, mida varem tuli vaadelda eeskätt infoühiskonna ning e-kaubanduse arengu ning üksikisiku õiguste kontekstis, tuleb nüüd vaagida ka lähtuvalt kõrgenenud ohust ühiskonnale, mis omakorda võib tasakaalu kaubanduse ja üksikisiku huvide vahel nihutada. Tõlgendamise abil saab õiguse mõte

täpsema ja selgema sisu ning annab seeläbi vastuse küsimustele, mida varasemas ohuolukorras ja sündmustikus polegi olnud põhjust esitada.

Kolmandas peatükis pakub autor välja küberjulgeoleku õiguse temaatilise ja analüütilise raamistiku, esitades omapoolse vaate küberjulgeoleku tagamise seisukohalt olulisematele küsimustele ning õiguslikud lähtekohad neile vastamiseks. Autor kasutab esimese ja teise peatüki analüüsi toomaks välja enim vaieldud ja toonitatud probleemvaldkonnad – territoriaalsuse põhimõtte rakendatavus küberjulgeoleku regulatsioonile tervikuna, küberintsidentide toimepanijate tuvastamine ning sellega seonduvad vastutusele võtmise probleemid, rahvusvahelise ja avaliku ning erasektori koostöö võimalikkus ja reglementeeritus, enesekaitse teostamise eeldused küberintsidentide korral, teabevahetuse privaatsusõiguslikud ning infovabaduslikud aspektid, samuti kriminaalõiguse ühtlustamise problemaatika ning vajadus täpsustada erinevate asutuste ja rahvusvaheliste organisatsioonide pädevust küberjulgeoleku tagamisel. Autor viitab rahvusvahelisest õigusest ja riikide hiljutisest õiguspraktikast, aga ka teooriakirjandusest tulenevatele õiguslikele alustele kõnealuste probleemide lahenduse lähtekohana ning selgitab vajadust erinevate õigusvaldkondade teoreetilise ja praktilise käsitluste ühtlustamise või vähemalt nende seostatud analüüsi järele.

Autor käsitleb iga probleemvaldkonda esmalt läbi selle põhiprobleemide ja –küsimuste ning neile vastavate ekspertseisukohtade, toonitades vajadusel seisukohtade erinevusi või praktilisi probleeme nende rakendamisel. Seejärel tuletab autor valitud teemadega seonduvate põhiseisukohtade pinnalt kontseptsiooni rahvusvahelisel tasandil kehtivatest küberjulgeolekut toetavatest reeglitest, mille eesmärgiks on arendada ekspertdiskussiooni teemal, millises ulatuses ja milliste eranditega antud reeglid kaasagsele küberjulgeolekuolukorrale kohaldatavad on.

Autor väidab, et kujunemisjärgus rakendus- ja tõlgenduspraktika ei võimalda täna asuda seisukohale, et õiguslikud alused küberjulgeoleku tagamiseks puuduvad. Küll aga võimaldab kehtiv rahvusvaheline õigus ning hiljutine rakenduspraktika arendada kontsentreeritud diskussiooni küsimuses, millises ulatuses on küberjulgeolekut võimalik kehtiva õiguse pinnalt tagada. Sellise arutelu tulemusena on võimalik kaardistada ka tegelikud lüngad ning otsustada, millisel tasandil tekib vajadus täiendava õigusloome järele.

Doktoritöö on kirjutatud kontseptuaalsel tasandil, kuid selle raames on autor viinud läbi küberjulgeolekuga seonduvate rahvusvaheliste õigus- ja poliitiliste instrumentide analüüsi ning koostanud rahvusvaheliste kohtute lahendite ülevaatematerjali. Arvestades töö peamist eesmärki, milleks on õigusekspertidele küberjulgeoleku valdkonna regulatsiooni ning analüüsi raamistiku konstrueerimine, on autor tuvastatud materjali loendi esitanud käesoleva väitekirja lisadena. Autor ei ole pidanud vajalikuks esitada kokkuvõtet instrumentidest ja lahenditest töös, kuivõrd väitekirja peamine järeldus on, et kehtiv õigus ning õiguspraktika vajavad läbivaatamist lähtuvalt muutunud küberjulgeoleku olukorrast nii riikides kui maailmas tervikuna ning selle teostamine eeldab erinevate õigusvaldkondade ning ekspertiisi kombineerimist. Autor on

seisukohal, et õiguses tekkinud tõlgenduslikke erimeelsusi ei ole võimalik ületada laiapõhjalisema aruteluta, kuivõrd iga üksiku eksperdi, aga ka õigusvaldkonna vaated ja ettevalmistus ei ole piisav laiapõhjalise küberkaitse vajaduste mõistmiseks ja arvestamiseks.

Kui õiguse areng tervikuna on loomulik nähtus, siis küberjulgeoleku kontekstis on see kujunenud omamoodi probleemiks, mida rahvusvahelisel tasandil on hakatud pidama lausa üheks olulisimaks piiranguks küberturvalisuse tagamisele. Mitmed riigid on asunud seisukohale, et uue rahvusvahelise kokkuleppeta pole küberjulgeoleku tagamine võimalik, kuivõrd kehtiv rahvusvaheline õigus ei ole loodud tänast ohuolukorda ja võimeid arvestades. Autor selgitab, et vaatamata faktile, et ükski rahvusvahelise õiguse instrument ei ole loodud vahetult laiapõhjalise küberjulgeoleku vajadustest lähtuvalt, on rahvusvahelisel tasandil vastu võetud hulk instrumente, mis katavad erinevaid küberjulgeoleku aspekte nagu infoühiskonna areng tervikuna, andmevahetus, koostöö intsidentide ennetamisel ja uurimisel, aga ka tegutsemine sõjalise iseloomuga küberrünnete korral. Probleemideks on eeskätt selliste õiguslike meetmete hajutatus (autor on tööle lisanud loendi küberjulgeoleku erinevaid teemasid käsitlevatest instrumentidest) nii allikate kui õigusvaldkondade vahel ning erinevatesse õigusvaldkondadesse kuuluvate õigusinstituutide seoselise tõlgendamise ja kohaldamise praktika puudumine. Muuhulgas tuleb õigust leida instrumentidest, mis pole algselt suunatud küberjulgeolekule, vaid julgeolekule laiemalt (nt sõjaõiguse ning terrorismivastase võitluse instrumendid).

Arvukate ekspertarutelude ja konverentside pinnalt toob autor välja sagedasemad õiguslikku käsitlust vajavad küberjulgeoleku probleemid ning neist igaühele vastava kehtiva õigusliku raamistiku. Seeläbi soovib autor juhtida nii erineva spetsialiseeritusega juristide kui küberjulgeoleku tagamise seotud teiste ekspertvaldkondade esindajate diskussiooni senisest enam kõneluste õiguslike kontseptsioonide (territoriaalsuse põhimõte, vastutus rahvusvahelise õiguse rikkumise eest, rahvusvahelise koostöö korraldus, enesekaitse, andevahetus, teabele juurdepääs, hoolsuskohustus, kriminaliseerimine ning kriminaalpoliitika ja riiklike ning rahvusvaheliste küberjulgeoleku tagamisega seotud asutuste ja organisatsioonide pädevus) ulatuse, erandite ning kokkuvõttes õiguskorras tegelikult eksisteerivate lünkade ja võimaliku normikonkurentsi väljaselgitamiseni.

Autor on mitmeid töös käsitletud teemasid sügavamalt avanud teadusartiklites, mida samuti on töös refereeritud vähimas võimalikus mahus vältimaks töö abstraktsioonitaseme kõikumist autori enda ekspertiisiga kaetud teemades.

Artikkel „*Applicability of the Census Case in Estonian Personal Data Protection Law*“, avaldatud kaastöös Monika Mikiver'iga ajakirjas „*Juridica International*“ aastal 2006 vaatleb laiemalt vajadust hinnata õiguslike mõjusid ning rakendupraktikat konkreetse jurisdiktsiooni ning asjaolude valguses. Artiklis selgitatakse, et Eesti andmekaitseõiguse kujundamisel ei tohiks lähtuda üksnes Saksa õigusteooriast ja –praktikast, kuivõrd infoühiskonna arengu põhimõtted ning valdkonna ajalooline kujunemine on kahes riigis olulisel määral erinevad. Artiklis „*Legal and Policy Evaluation: International Coordination of Pro-*

secution and Prevention of Cyber Terrorism“ (2007) asuvad käesoleva dissertatsiooni autor ning Reet Oorn seisukohale, et küberterrorism ei ole vaatamata sellekohase termini laialdasele kasutamisele meedias, täna õiguse rakendamise keskpunkt, kuivõrd kaasaegsete küberrünnete näol on tegemist riigi julgeoleku valdkonda kuuluvate intsidentidega laiemalt, millega ei tegele niivõrd rahvusvahelised terrorismi levikut piiravad instrumendid kui riigisisene õigus. Arvestades autori peamist ekspertiisivaldkonda, on privaatsuse kaitsega seonduvaid küberjulgeleku probleeme vaadelduda kahes artiklis: 2009. a. ilmunud „*Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective*“ ja 2010.a. avaldatud „*IP-Addresses as Personal Data*“. Nendes artiklites käsitleb autor lähemalt uut tasakaalu ning sellest lähtuvat tõlgenduspraktika muutust küberjulgeolekuintsidentide alase infovahetuse ja üksikisiku eraelu kaitse vajaduste vahel.

Artiklites „*Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons*“ (2010) ja „*Developments in the Legislative, policy and Organisational Lanscapes in Estonia since 2007*“ (2010) käsitleb autor koos Kadri Kaska ja Anna-Maria Talihärm’iga lähemalt Eestit 2007.a. tabanud poliitilise kontekstiga küberrünnete ulatust ning nende lahendamiseks võetud meetmeid. Kirjutises „*Global Cyber Security – Thinking About Ways Ahead for NATO*“ ajakirjale „*SAIS Review*“ pakub autor välja käsitluse laiapõhjalisest lähenemisest küberjulgeolekule Põhja-Atlandi Lepingu Organisatsiooni eesmärke ja ülesandeid silmas pidades.

Samuti on autor kaastöös teiste ekspertidega süvitsi vaadelnud kübervaldkonna heidutuse ja kollektiivse kaitse temaatikat (ajakirkas IEEE ilmunud artiklis “*From Chaos to Collective Defense*”, 2010) ning võimalikke analoogiaid küberjulgeolekuga seonduvate õiguslünkade ületamiseks (“*Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation*”). Kõnealuseid artikleid ei ole nende kogumahu tõttu käesolevale tööle lisatud, kuid autor on need kättesaadavaks teinud interneti vahendusel.

BIBLIOGRAPHY

Referred Literature

1. **Adkins, Bonnie N.** The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role? A research report submitted to the faculty in partial fulfilment of the graduation requirements. Alabama, 2001.
2. **Ala-Mutka, Kirsti** et al. The Impact of Social Computing on the EU Information Society and Economy. Institute of Prospective Technological Studies, European Commission (2009).
3. **Aldrich**, **Richard W.** Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime. INSS Occasional Paper 32, Information Operations Series, 2000.
4. **Aldrich**, **Richard W.** The International Legal Implications of Information Warfare. Airpower Journal. 1996
5. **Alexander, Keith B.** Warfighting in Cyberspace. Joint Forces Quarterly. Iss. 46, 2007.
6. **Altford, Lionel**. Cyber Warfare: Protecting Military Systems. Acquisition Review Quarterly, Spring 2000
7. **Andjelkovic**, **Maja.** Internet Governance: In the Footsteps of Global Administrative Law. University of Kent Law School. September (2006).
8. **Antolin-Jenkins**, **Vida M.** Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places? Naval Law Review. Vol. 51, 2005.
9. **Archick**, **Kristin.** Cybercrime: The Council of Europe Convention. CRS Report for Congress, 22 July 2004.
10. **Arquilla, John and Ronfeldt, David.** Cyberwar is Coming. Santa Monica, CA: RAND Corporation, 1993
11. **Barlow**, **John Perry.** A Declaration of the Independence in Cyberspace. 8 February 1996.
12. **Barrett, Larry**. US Reviewing Cyber Threat to Power Grid.
13. **Benatar, Marco**. The Use of Cyber Force: Need for Legal justification? In Goettingen Journal of International Law I (2009)
14. **Blair, Stephanie**. Towards Integration? Unifying Military and Civilian ESDP Operations. European Security Review. No. 44, May 2009.
15. **Blakely**, **Rhys** et al.. MI5 alert on China's cyberspace spy threat. The Times, 1 December 2007.
16. **Blume, Peter**. Information Infrastructure and Data Protection. The Danish perspective. International Journal of Law and Information Technology, Vol. 4 No. 1
17. **Borg, Scott**. The Cyber-Defense Revolution – A Synthesis, 2009.
18. **Bowcott**, **Owen.** "Cyber crime costs the UK more than £27bn a year". The Guardian, 17 February 2011.
19. **Brenner, Susan and Dion, Maeve**. Civilians in Information Warfare: Conscription of Telecom Networks and State Responsibility for International Cyber Defense. Proceedings of ICIW 2010. The 5th International Conference on Information-Warfare & Security (2010).
20. **Broadhurst**, **Roderic.** Developments in the Global Law Enforcement of Cyber Crime. International Journal of Police Strategies and Management. Vol. 29, Issue. 3.

21. **Brown**, **Davis.** A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. Harvard Int. Law Journal. Vol. 47, No. 1, 2006.
22. **Brown, Davis**. Use of Force against Terrorism after September 11th: State Responsibility, Self-Defense and Other Responses. 11 Cardozo J. Int'e & Comp. L. 1. Spring, 2003.
23. **Brown, Davis**. Use of Force against Terrorism after September 11th: State Responsibility, Self-Defense and Other Responses. 11 Cardozo J. Int'e & Comp. L. 1. Spring, 2003.
24. **Brownlie, Ian**. International Law and the Use of Force by States (1963);
25. **Bygrave, Lee A**. Data Protection Law: Approaching Its Rationale, Logic and Limits. Kluwe Law International, 2002
26. **Carr, David**. Five Things You Need To Know About IPv6. Computerworld, August 31, 2010.
27. **Carr, Jeffrey**. Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, 2009.
28. **Castells**, **Manuel.** The Information Age. Economy, Society, and Culture. Vol. 1–3. Wiley-Blackwell, 2010.
29. **Cavelty, Myriam**. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge (2008).
30. **Cavelty**, **Myriam.** Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. Journal of Information Technology and Politics. Vol. 4, No. 1, 2007.
31. **Cavelty**, **Myriam.** Critical Information infrastructure: Vulnerabilities, Threats and Responses. Geneva: United Nations Institute for Disarmament Research, 2007.
32. **Chabinsky, Steven R.** Cybersecurity Strategy: A Primer for Policy Makers and those on Front of the Line. Journal of National Security Law and Policy. Vol. 4, No. 1, 2010.
33. **Chik, Warren B.** Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore, 2007.
34. **Clay, Wilson**. CRS Report for Congress: Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.
35. **Clayton, Richard**. Complexities in Criminalizing Denial of Service Attacks. http://www.cl.cam.ac.uk/~rnc1/complexity.pdf.
36. **Clove**, **Charles.** Kremlin-backed group behind Estonia cyber blitz. Financial Times, 11 March 2009.
37. **Coalson**, **Robert.** Behind The Estonia Cyberattacks. RFE/RL, 6 March 2009.
38. **Condron**, **Sean M.** Getting it Right: Protecting American Critical Infrastructure in Cyberspace. Harvard Journal of Law & Technology. Volume 20, Number 2, Spring 2007.
39. **Cornish**, **Paul.** Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Directorate-General for External Policies of The Union, European Parliament, 2009.
40. **Cornish, Paul, Hughes, Rex and Livingstone, David**. Cyberspace and the National Security of the United Kingdom. Threats and Responsess. Chatham House: A Chatham House Report. 2009.

41. **Cox, Noel**. The Regulation of Cyberspace and the Loss of National Sovereignty. Socio-Legal Studies Association, 2002 Annual Conference University of Wales Aberystwyth, United Kingdom 3–5 April 2002.
42. **D'Amato, Anthony**. International Law, Cybernetics, and Cyberspace. In: Computer Network Attack and International Law. Michael N. Schmitt & Brian T. O'Donnell eds., 2002.
43. **Davis**, **Joshua.** Secret Geek A-Team Hacks Back, Defends Worldwide Web. Wired, 24 November 2008.
44. **Denning, Dorothy E.** A View of Cyberterrorism Five Years Later. Readings in Internet Security: Hacking, Counterhacking, and Society (K. Himma ed.), Jones and Bartlett Publishers, Boston, 2006.
45. **Denning**, **Dorothy E.** Barriers to Entry: Are They Lower for Cyber Warfare? IO Journal, April 2009.
46. **Denning**, **Dorothy E.** Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives. 2000.
47. **Denning**, **Dorothy E.** Information Warfare and Security. Addison-Wesley, 1999.
48. **Denning**, **Dorothy E.** Cyber Conflict as an Emergent Social Phenomenon. In: Thomas J. Holt (Ed.), Bernadette H. Schell (Ed.) Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (2011).
49. **DeZwart**, **Melissa.** The Future of the Internet: Content Regulation and its Potential Impact on the Shape of Cyberspace. Entertainment Law Review, Volume 9 Issue 2, February 1998.
50. **Dickie, John**. Internet and Electronic Commerce in the European Union. Oxford, Portland Oregon: Hart Publishing, (1999).
51. **Dignan**, **Larry**. China's Cyber-Militia Behind US blackouts.
52. **Dinstein, Yoram**. War, Aggression and Self-Defence. Cambridge University Press, 4th Edition, 2005.
53. **Dobrzeniecki**, **Karol.** How Should We Deal with Human rights in Cyberspace? Some Remarks. International Review of Law Computers & Technology, Vol. 19, No. 3, November 2005.
54. **Drummer**, **Alan.** Cyber 9/11. How Do We Prevent It? Symantech CIO Online Digest Extra. November 2009.
55. **Dylevskii, I. N. and Komov, S.A.** et al. Russian Federation Military Policy for Provision of International Information Security. Military Thought 2006.
56. **Easterbrook, Frank.** Cyberspace and the Law of the Horse. University of Chicago Legal Forum 1996.
57. **Esposito, G.** The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument? Broadhurst, R. Ed, Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong, 2004.
58. **Evron, Gadi**. Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War. Georgetown Journal of International Affairs. Winter/Spring 2008.
59. **Eyden, J.** France blames China for hack attacks. The Register, September 12, 2007.
60. **Ferrera, Gerald R.** et al. Cyberlaw: Texts and Cases. Thomson Publishing, 2nd Ed., 2004.
61. **Froomkin**, **Michael.** Cybercrime Treaty Goes Live. Discourse.net, 19 March 2004.
62. **Gable**, **Kelly A.** Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent.

63. **Geers**, **Kenneth**. Cyberspace and the Changing Nature of Warfare. SCMagazine, 27 August 2008.
64. **Geers, Kenneth**. The Challenge of Cyber Attack Deterrence. Computer Law & Security Review March, 2010.
65. **Geers, Kenneth**. Strategic Cyber Security. CCD COE Publishing 2011.
66. **Gercke**, **Marco.** Europe's Legal Approaches to Cybercrime. ERA Forum. Vol. 10, No. 3, 2009.
67. **Girasa**, **Roy J.** Cyberlaw: National and International Perspectives. Prentice Hall,, 2002.
68. **Goldman, Eric.** Teaching Cyberlaw. Santa Clara University School of Law Legal Studies Research Papers Series. Paper No. 08–57, July 2008.
69. **Goodin**, **Dan.** India and Belgium decry Chinese cyber attacks. The Register, 8 May 2008.
70. **Goodin, Dan.** Pentagon attackers stole 'amazing amount' of sensitive data. The Register, March 6, 2008.
71. **Goodman, Marc D. and Brenner, Susan W.** The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology, Vol. 10, No. 2, 2002.
72. **Gotved, Stine**. Time and space in cyber social reality. New Media Society. Vol. 8, No. 3, June 2006.
73. **Green**, **Joshua.** The Myth of Cyberterrorism. Washington Monthly. November 2002.
74. **Greenberg**, **Lawrence T** et al. Information Warfare and International Law. National Defense University Press (1998).
75. **Grief**, **Nicholas.** EU Law and Security. E.L.Rev. (2007).
76. **Grimmelmann, James and Ohm, Paul**. Review of The Future of the Internet – and How to Stop It by Jonathan Zittrain, 2009.
77. **Habiger**, **Eugene E.** Cyberwarfare and Cyberterrorism: The Need for a New US Strategic Approach. The Cyber Secure Institute, 2010.
78. **Herrera, Geoffrey L**. Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space.m 1st International CISS/ETH Conference on „The Information Revolution and the Changing Face of International Relations and Security", May 23–25, 2005.
79. **Hirvonen**, **Timo and Frank**, **Lauri.** Measuring the Information Society in Europe: From Definitions to Description. ERSA conference papers, 2006.
80. **Hoeren**, **Thomas.** Was ist das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme"? Multimediarecht 2008.
81. **Hollis**, **Duncan B.** Why States Need an International Law for Information Operation. Lewis & Clark Law Review. Vol. 11, 2007.
82. **Hopkins**, **Shannon L.** Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, Vol II No. 1, 2003.
83. **Häußler, Ulf**. Ensuring and Enforcing Human Security: The Practice of International Peace Missions. War or Crime? National Legal Challenges in Europe to the War in Iraq. Wolf Legal Publishers, 2009.
84. **Hyppönen**, **Mikko.** Unrest in Estonia. F-Serucre, 2007.
85. **Jayawal V.** et al. Internet hack back: counter attacks as self-defense or vigilantism? IEEE 2002.
86. **Jennings, Robert, Watts Arthur (**Eds.). Oppenheim's International Law 33, 9th Ed., 1992.

87. **Jensen, Eric Talbot.** National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Stanford Journal of International Law. Summer 2002
88. **Johnson, David and Post, David**. Law and Borders – the Rise of Law in Cyberspace. 48 Stan. L. Rev. 1367,1370 (1996).
89. **Johnson**, **Phillip A.** "Is It Time for a Treaty on Information Warfare?" In International Law Studies, Vol. 76.
90. **Kaska, Kadri, Talihärm, Anna-Maria and Tikk, Eneken**. Developments in the Legislative, Policy and Organizational Landscapes in Estonia Since 2007. International Cyber Security Legal & Policy Proceedings. CCD COE Publishing, 2010.
91. **Katsch, Ethan**. Cybertime, Cyberspace and Cyberlaw. 1995 J. Online L. Article 1.
92. **Keyser**, **Mike.** The Council of Europe Convention on Cybercrime. Journal of Transnational Law & Policy, Vol 12:2, Spring 2003.
93. **Kierkegaard**, **Sylvia Mercado.** Cracking Down On Cybercrime Global Response: The Cybercrime Convention. Communications of the IIMA (2005).
94. **Kissel**, **Richard.** Glossary of Key Information Security Terms. National Institute of Standards and Technology (2006).
95. **Künnapu**, **Markko.** Council of Europe Convention on Cybercrime. European Union Framework Decision on attacks against information systems: Comparative study on the implementation and recent developments. A research paper for the Cooperative Cyber Defence Centre of Excellence (2008).
96. **Lachow**, **Irving.** Cyber Security: A Few Observations. National Defense University. 2008.
97. **Landler**, **Mark and Markoff**, **John.** In Estonia, What May be the First War in Cyberspace. International Herald Tribune, 28 May 2007.
98. **Leiner, Barry M** et al. A Brief History of the Internet. Internet Society, 1997.
99. **Lessig**, **Lawrence.** Code and Other Laws in Cyberspace. 1999
100. **Lessig, Lawrence**. Free Culture (2004) p. xiv. Available at http://www.free-culture.cc/freecontent/ (last accessed May 5, 2011).
101. **Lewis, James A**. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. CSIS, Washington, DC, December 2002.
102. **Leyden**, **John.** France blames China for hack attacks. The Register, 12 September 2007.
103. **Li, Xingan**. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene, 2007.
104. **Licklider**, **Joseph.** Man-Computer Symbiosis. IRE Transactions on Human Factors in Electronics. Volume HFE–1, March 1960.
105. **Licklider**, **Joseph.** The Computer as a Communication Device. Science and Technology. April 1968.
106. **Lorents Peeter, Ottis Rain and Rikk Raul**. Cyber Society and Cooperative Cyber Defence. In: Proceedings of HCI (14), (2009).
107. **Lorents, Peeter** *et al*. Cyber Security Situation in Estonia. Estonian Ministry of Defense, 2006. Document with restricted access
108. **Majuca, Ruperto P. and Kesan Jay P**. Hacking Back: Optimal Use of Self-Defence in Cyberspace. Illinois Public Law Research Paper No. 08–20, 18 March 2009.
109. **Manolopoulus, Andreas**. Raising Cyber-Borders: The Interaction Between Law and Technology. International Journal of Law and Information Technology, Vol. 11, No. 1.

110. **McMillan, Robert.** With unrest in Iran, cyber-attacks begin. NetworkWorld, June 15, 2009.
111. **Menon**, **Vineetha.** FBI: Cyber terrorism threat is 'rapidly expanding'. ITP Net, 2010.
112. **Meyer**, **David.** IPv4 addresses: Less than 10pc still available. ZDNet UK. 19 January 2010.
113. **Murray**, **Andrew D.** The Regulation of Cyberspace: Control in the Online Environment. Routledge-Cavendish, 2007.
114. **Murphy, Sean D**. The Doctrine of Preemptive Self-Defense. Villanova law Review, Volume 50, 2005
115. **Nissenbaum, Helen**. Where computer security meets national security. Ethics and Information Technology, 2005, No. 7
116. **Ohm**, **Paul.** The Myth of the Superuser: Fear, Risk, and Harm Online. University of Colorado Law School, 2007.
117. **Ophardt**, **Jonathan A.** Cyber Warfare and the Crime of Aggression: the Need for Individual Accountability for Tomorrow's Battlefield. Duke Law and Technology Review. No. 3, 2010.
118. **Orwell**, **George.** 1984. London: Secker & Warburg, 1949.
119. **Ottis, Rain**. From Pitchforks to Laptops: Volunteers in Cyber Conflicts. Conference on Cyber Conflict Proceedings 2010, C. Czosseck and K. Podins (Eds.). CCD COE Publications, 2010, Tallinn, Estonia.
120. **Polanski, Przemyslaw Paul.** Customary Law of the Internet: In Search for a Supranational Cyberspace Law. – TMC Asser Press. The Hague, 2007.
121. **Pellerin, Cheryl**. White House Launches US International Cyber Strategy. American Forces Press Service, May 17, 2011.
122. **Portnoy, Michael and Goodman**, **Seymour.** Global Initiatives to Secure Cyberspace: An Emerging Landscape. Springer, 2009.
123. **Posner**, **Erik P. and Lichtman**, **Douglas.** Holding Internet Service Providers Accountable. The Law and Economics of Cybersecurity. New York: Cambridge University Press, 2006.
124. **Radcliff**, **Deborah.** Can You Hack Back? CNN, 1 June 2000.
125. **Reich, Pauline**. Cybercrime, Cybersecurity, and Financial Institutions Worldwide. In: Cyberlaw for Global E-business: Finance, Payments and Dispute Resolution, 2008.
126. **Joel R. Reidenberg**. Lex Informatica: The Formulation of Information Policy Rules Threough Technology. Texas Law Review, Volume 76, N0. 3, February 1998.
127. **Rohrmann, Carlos Alberto**. The Role of the Dogmatic Function of Law in Cyberspace. International Journal of Liability and Scientific Enquiry, Vol. 1, No. 1–2 / 2007.
128. **Rosenstock, Robert.** The ILC and State Responsibility. 96(4) AJIL 792, 2002.
129. **Rudesill, Dakota S**. Precision War and Responsibility: Transformational Military Technology and the Duty of Care under the Laws of War. The Yale Journal of International Law. Summer 2007
130. **Ryan, Julie, Ryan, Daniel and Tikk Eneken**. Cyber Security Regulation: Using Analogies to Develop Frameworks for regulation. In: International Cyber Security Legal and Policy Proceedings, CCD COE 2010.
131. **Schachtman**, **Noah.** Cybersecurity: Here's What Really Worries the Pentagon. Wired, 2010.

132. **Schjølberg**, **Stein and Ghernaouti-Hélie**, **Solange.** A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace. Cybercrimedata, 2009.
133. **Schjolberg**, **Stein.** A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime. United Nations (2010).
134. **Schmitt**, **Michael N.** Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law. Vol. 37, 1998–99.
135. **Schmitt, Michael N**. Bellum Americanum: The US View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict. 19 Mich. J. Int'l L. 1081, 1998.
136. **Schultz**, **Thomas.** Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Publi International Law Interface. The European Journal of International Law Volume 19 Number 4, 2008.
137. **Schonfeld**, **Erick.** Russia Is Rising in Internet Population. TechCrunch, 27 August 2008.
138. **Selleck**, **Evan.** IBM z196 5.2GHz CPU Breaks Records, Could Cost Hundreds of Thousands. Slashgear, 25 August 2010.
139. **Sevastopulo, D. and McGregor, R**. Chinese military hacked into Pentagon. September 3, 2007.
140. **Sharp, Walter G**. Cyberspace and the Use of Force. 1999,
141. **Sieber, Ulrich** et al. Cyberterrorism – the use of the Internet for terrorist purposes. Council of Europe Publishing, (2007).
142. **Sieber**, **Ulrich.** Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study. University of Würzburg (1998).
143. **Sklerov**, **Matthew J.** Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent. In: 201 MIL. L. REV. (1–85) 2009.
144. **Sommer, Joseph**. "Against Cyberlaw." Berkeley Technology Law Journal, Fall 2000.
145. **Sosa, Gilbert C.** Country Report on Cybercrime: The Philippines (2010).
146. **Standage**, **Tom.** The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers. Walker & Company 1998.
147. **Stoll**, **Clifford.** The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage. Doubleday, 1989.
148. **Streltsov**, **A. A.** International Information Security: Description and Legal Aspects. In: Disarmament (Vol. 3), 2007.
149. **Talihärm**, **Anna-Maria.** Cyber Terrorism: in Theory or in Practice? CCD COE Publishing, 2011.
150. **Talihärm, Anna-Maria.** Defining Cyberterrorism. LLM thesis of Stockholm University, 2008.
151. **Tikk, Eneken and Nõmper, Ants**. Informatsioon ja Õigus. Tallinn: Juura, 2007.
152. **Tikk, Eneken and Mikiver, Monika**. Applicability of the Census Case in Estonian Personal Data Protection Law. Juridica International, 1, 2006.
153. **Tikk, Eneken and Kaska, Kadri**. Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. ECIW Proceedings 2010.
154. **Tikk, Eneken, Talihärm, Anna-Maria**. Cyber Security in European Union Legal and Policy Documents, p. 18. CCD COE Publishing, 2008

155. **Tikk, Eneken**. IP Addresses Subject to Personal Data Regulation. In: International Cyber Security Legal and Policy Proceedings. CCD COE Publications 2010.
156. **Tikk, Eneken.** Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective, in: NATO Science for Peace and Security Series – E: Human and Societal Dynamics, "Modelling Cyber Security: Approaches, Methodology, Strategies", IOS Press, Volume 59, 2009.
157. **Tikk**, **Eneken**. Frameworks for International Cyber Security: Legal and Policy Instruments. CCD COE Publishing, 2010.
158. **Tikk**, **Eneken.** Frameworks for International Cyber Security: National Cyber Security Strategies. CCD COE Publishing, 2011.
159. **Tikk**, **Eneken.** Global Cyber Security – Thinking About Ways Ahead for NATO. SAIS Review of International Affairs, will be published late 2010.
160. **Tikk, Eneken; Kaska, Kadri and Liis Vihul**. International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence, 2010.
161. **Turk**, **Robert J.** Cyber Incidents Involving Control Systems. Idaho National Laboratory, 2005.
162. **Vanhamme, Jan**. Formation and Enforcement of Customary International Law: the European Union's Contribution. Netherlands Yearbook of International Law (2008), 39, pp. 127–154
163. **Veerasamy N. and Taute, N**. An Introduction to Emerging Threats and Vulnerabilities to Create User Awareness. Council for Scientific and Industrial Research, 2009.
164. **Vixie**, **Paul.** Cyberterrorism isn't so much a threat to national security as a threat to civilisation. Newsweek, 2003.
165. **Vogel**, **Joachim.** Towards a Global Convention against Cybercrime. First World Conference on Penal Law. Penal Law in the 21st Century, 2007.
166. **Walker, Allen D**. Applying International Law to the Cyber Attacks in Estonia. April 2008.
167. **Weimann**, **Gabriel.** Cyberterrorism: How Real Is The Threat? Special Research Report, Washington DC: United States Institute of Peace, 2004 .
168. **Weiner**, **Tim.** The Man Who Protects America from Terrorism. New York Times, 1 February 1999.
169. **Weiss, Joe.** "The Need for Interdisciplinary Programs for Cyber Security of Industrial Control Systems", WorldComp, 2010.
170. **Westby, Jody**. Homeland Security v Homeland Defense: Gaps Galore. Paper for St. Mary's Universiry School of Law, Center for Terrorism Law Seminar „State Open Government Law and Practice in a Post–9/11 World: Legal and Policy Analysis. November 2007.
171. **Westin, Alan F**. Social and Political Dimensions of Privacy. Journal of Social Issues, Vol. 59, No. 2, 2003
172. **Wingfield, Thomas C. and Michael**, **James B.** An Introduction to Legal Aspects of Operations in Cyberspace. Technical Report NPS-CS–04–005, Naval Post-graduate School, Department of Computer Science, Monterey, California, 28 Apr. 2004.
173. **Wingfield Thomas C. and Tikk Eneken**. Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen. In: International Cyber Security Legal and Policy Proceedings. CCD COE Publications 2010.
174. **Wulf William A. and Jones Anita K.** Cybersecurity. National Academy of Engineering Publications, Vol. 32, No. 1, March 2002.

Referred Policy Documents

175. Principles of Estonian Information Policy 2004–2006.
176. The Strategy on the Development of the Information Society in Poland for the years 2004–2006.
177. Strategy of the Republic of Slovenia in the Information Society.
178. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM (2009) 149).
179. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime (COM (2000) 890).
180. Hungarian Information Society Strategy. Informatikai és Hírközlési Minisztérium.
181. Information Society Strategy and Annexed Action Plan. State Planning Organization. 2006.
182. Declaration of Principle. Building the Information Society: a global challenge in the new Millennium. World Summit on the Information Society, 2003.
183. Cyber Security Strategy. Estonian Ministry of Defence, 2008.
184. Cyber Security Strategy of the United Kingdom. 2009.
185. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach (COM (2001) 298).
186. Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008.
187. Note by Secretary General "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (A/65/201), 30 July 2010.
188. Decision no. 991 OSCE conference on a comprehensive approach to cyber security: exploring the future OSCE role. PC.DEC/991, 31 March 2011.
189. NATO Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002.
190. NATO Riga Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006.
191. North Atlantic Treaty. Washington D.C., 4 April 1949.
192. NATO 2020: Assured Security; Dynamic Engagement. 17 May 2010.
193. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions on Towards a general policy on the fight against cyber crime (COM (2007) 267) final.
194. Opinion of the Committee of Experts on Terrorism (CODEXTER) on cyberterrorism and use of Internet for terrorist purposes. Strasbourg: The Cybercrime Convention Committee (T-CY), 12 March 2008, document T-CY (2008) INF 02 E.
195. Council of Europe Project on Cybercrime Final Report. Strasbourg: Economic Crime Division of the Directorate General of Human Rights and Legal Affairs, 14 May 2009. Document ECD/567(2009)1.

196. OECD MC.DEC/7/06.
197. Report by the OSCE Secretary General on the Implementation of MC.DEC/2/09 on Further OSCE Efforts to Address Transnational Threats and Challenges to Security and Stability.
198. US proposal „An OSCE Strategy for a Comprehensive Approach to Cyber-security“ March 1, 2011.
199. Explanatory Report to the Council of Europe Cybercrime Convention (ETS 185).
200. US Proposal for an OSCE Strategy for a Comprehensive Approach to Cyber-security (Draft as of March 1, 2010), p. 3.
201. EU-US Summit Joint Statement. Lisbon, 20 November 2010.
202. ITU Toolkit for Cybercrime Legislation. February 2010.
203. Principles of Estonian Information Policy. Estonian Parliament, 1998.
204. Strategy to improve Internet security in Sweden. 2006, pp. 59–67.
205. NATO Cyber Defense Policy. 20 December 2007. Document with restricted access.
206. NATO Cyber Defense Concept. 13 March 2008. Document with restricted access.
207. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty. UNGA Resolution 2131 (1965).
208. G.A. Res. 2625, at 121, 124, U.N. GAOR, 25th Sess., Supp. No. 28 (Oct. 24, 1970).
209. G.A. Res. 1514, at 67, U.N. GAOR, 15th Sess., Supp. No. 16, U.N. Doc. A/4684A (Dec. 14, 1960).
210. OECD Work on Spam, 2004
211. Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. World Summit on the Information Society, 2003

Referred International Legal Instruments

212. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), 17.7.2000 EN L 178/1 Official Journal of the European Union. OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam, 2006.
213. Directive 2006/24/EC 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. (Data retention directive).
214. Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Also Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.
215. Directive 98/48/EC of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. OJ L 217/18 05.08.1998. Recital 6.
216. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 , 23/11/1995.

217. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201 , 31/07/2002.
218. Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.
219. Framework Decision 2005/222/JHA of 17 January 2005 on attacks against information systems.
220. The Council of Europe Convention on Cybercrime (ETS 185, signed on 23 November 2001, entry into force on 1 July 2004)
221. International Telecommunication Convention. Concluded at Nairobi, 6 November 1982.
222. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.1981.
223. The European Convention on Human Rights, Rome 4 November 1950.
224. Estonian Public Information Act (RT I 2000, 92, 597)
225. Charter of the United Nations.
226. International Law Commission. Draft articles on Responsibility of States for Internationally Wrongful Acts 2001.
227. Agreement on Mutual Legal Assistance and Legal Relations in Civil, Family and Criminal Matters, signed on 26 January 1993. RT (State Gazette) II 1993, 16, 27; RT II 2002, 14, 58.
228. *European Convention on Mutual Assistance in Criminal Matters*, signed on 20 April 1959, Strasbourg

Other Sources

229. http://www.internetworldstats.com
230. http://www.worldmapper.org
231. http://www.pcmag.com (PCMAG encyclopedia)
232. http://www.merriam-webster.com (Merriam-Webster Dictionary)
233. http://www.ssa.gov (US Government Information Exchange Glossary)
234. http://csrc.nist.gov (NIST Glossary of Key Information Security Terms)
235. http://eur-lex.europa.eu (EUR-Lex Database)
236. http://www.riigiteataja.ee (Riigi Teataja)
237. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf Department of Defense Dictionary of Military and Associated Terms
238. http://www.nato.int/ NATO Official Website

Corporate Analysis
239. BitDefender. Conficker – One Year After. White Paper (2010).
240. Focal Report 3: Critical Infrastructure Protection. Cybersecurity – Recent Strategies and Policies: An Analysis. Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich. Zurich, 2009.
241. Unsecured Economies: Protecting Vital Information. McAfee, January 21, 2009, http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html (last accessed May 5, 2011).
242. National Cyber Security Research and Development Challenges, I3P, 2009.

Presentations
243. **Nemanja Malicevic**. Recent Initiatives and Plans at the OSCE. Presentation at CCD COE Conference on Cyber Conflict, Tallinn, 17 June 2010.
244. **Wolff Heintschel von Heinegg**. CCD COE Cyber Conflict Conference presentation 2010.

Reports
245. **James A. Lewis** et al. Securing Cyberspace for the 44th Presidency. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington: 2008
246. Cyber Security: What Role for CFSP? EU Institute for Security Studies Report. 10 March 2009
247. **Sverre Myrli**. Report "173 DSCFC 09 E bis – NATO and Cyber Defense" of 2009 Annual Session
248. **Klimburg, Alexander; Tiirmaa-Klaar, Heli**. Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU. European Parliament 2011
249. NATO 2020: Assured Security; Dynamic Engagement. 17 May 2010

Case Law
250. Nicaragua vs. United States of America), 1986 ICJ Rep. 14
251. Tadic Case (I.C.T.Y. Case # IT-94–1
252. Eastern Transport. CO.; New England Coal & Coke CO. v. Northern Barge Corporation; Hartwell & Son, Inc., v. Same 53 F.2d 107; 1931 US Dist. LEXIS 1744; Eastern Transport. CO.; New England Coal & Coke CO. v. Northern Barge Corporation; Hartwell & Son, Inc., v. Same 60 F.2nd 737 (U. S. Ct. App., 2nd Circuit, 1932). Cert. denied 287 US 662; 53 S. Ct. 220; 77 L. Ed. 571; 1932 US LEXIS 387 (1932)

Other
253. White House Press Briefing by Chief of Staff John Podesta, Secretary of Commerce Bill Daley, James Madison University President Linwood Rose and National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Dick Clarke on January 7, 2000.

Annex 1. Table of Definitions

Computer Network Attack (CNA)	Computer Network Attack aka Cyber warfare – using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability, while protecting one's own. (Cyberpower and National Security. Franklin d. Kramer, Stuart H. Starr, Larry K. Wentz; 2009)
-"-	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Joint Publication 1–02, DOD Dictionary of Military and Associated Terms)
Computer Network Exploitation (CNE)	Computer Network Exploitation – exploiting vulnerabilities in infrastructure systems, such as backbone routers or DNS servers to organize large-scale attack. The software at the heart of major infrastructure devices may have bugs or flaws; most are mere annoyances, but attackers might deliberately trigger some flaws to harm the system. Software programs to trigger such vulnerabilities are known as exploits. (Cyberpower and National Security. Franklin d. Kramer, Stuart H. Starr, Larry K. Wentz; 2009)
-"-	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (Joint Publication 1–02, DOD Dictionary of Military and Associated Terms)
Computer Network Defence (CND)	Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (Joint Publication 1–02, DOD Dictionary of Military and Associated Terms)
Computer Network Operations (CNO)	Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (Joint Publication 1–02, DOD Dictionary of Military and Associated Terms)
Computer security	Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. (Defending Your Digital Assets. Randall K. Nichols; Daniel J. Ryan; Julie J.C.H Ryan)
Cyberattack	An attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality, as applicable. (Defending Your Digital Assets. Randall K. Nichols; Daniel J. Ryan; Julie J.C.H Ryan)

	Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e. cyber security. (Australian Cyber Security Strategy 2010)
-"-	An offensive use of a cyber weapon intended to harm a designated target. (East-West Institute. Cybersecurity Critical Terminology Foundations. April 2011).
Cyber crime	The use of cyberspace for criminal purposes as defined by national or international law. (East-West Institute. Cybersecurity Critical Terminology Foundations. April 2011).
Cyber Defense	Organized capabilities to protect against, mitigate from, and rapidly recover from the effects of cyber attack. (East-West Institute. Cybersecurity Critical Terminology Foundations. April 2011).
Cyber war	An escalated state of cyber conflict between or among states in which cyber attacks are carried out by state actors against cyber infrastructure as part of military campaign. (East-West Institute. Cybersecurity Critical Terminology Foundations. April 2011).
Cyberspace	A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. (Cyberpower and National Security. Franklin d. Kramer, Stuart H. Starr, Larry K. Wentz; 2009, page 28)
-"-	The physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks; and their computer programs, computer data, content data, traffic data, and users. (ITU)
-"-	Cyber space encompasses all forms of networked, digital activities, this included the content and actions conducted through digital networks. (UK Cyber Security Strategy 2009)
-"-	The interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries. (NSPD54/HSPD 23). The virtual environment of information and interactions between people. (USA)

	An electronic medium through which information is created, transmitted, received, stored, processed and deleted. (East-West Institute. Cybersecurity Critical Terminology Foundations. April 2011).
Cybersecurity	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means. (Australia)
-"-	Cyber security embraces both the protection of [national] interests in cyber space and also the pursuit of wider [national] security policy through exploitation of the many opportunities that the cyber space offers. (UK Cyber Security Strategy 2009)
-"-	A property of cyber space that is an ability to resist to intentional and unintentional threats and respond and recover. (East-West Institute. Cybersecurity Critical Terminology Foundations. April 2011).
Information Security	Information security – Technical security measures that involve communications security, cryptography, and computer security. (Defending Your Digital Assets. Randall K. Nichols; Daniel J. Ryan; Julie J.C.H Ryan)
Network security	The protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects. (Defending Your Digital Assets. Randall K. Nichols; Daniel J. Ryan; Julie J.C.H Ryan)

Annex 2. International Cyber Security Law and Policy Instruments

Council of Europe

1. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)
2. Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows (2001)
3. Convention on Information and Legal Co-operation Concerning "Information Society Services" (2001)
4. Convention on Cybercrime (2001)
5. Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2002)

European Union

6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
7. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signature,
8. Communication 2000/0890 from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.
9. Council Resolution of 2000/C 293/02 on the organisation and management of the Internet
10. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).
11. Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
12. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Information Society Directive).
13. Communication 2001/0298 from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach.
14. Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security.
15. Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).

16. Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive).
17. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
18. Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).
19. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
20. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.
21. Communication 2004/0028 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or 'spam'.
22. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
23. Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies.
24. 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.
25. Communication 2006/0251 from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions – A strategy for a Secure Information Society – "Dialogue, partnership and empowerment".
26. Communication 2006/0661 from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions – Communication on the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies (Safer Internet plus).
27. Communication 2006/0688 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software
28. Communication 2006/0786 from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP)
29. Communication 2007/0267 from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime
30. Communication 2009/0149 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

31. Communication 2009/0064 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Final evaluation of the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies

Group of Eight

32. Meeting of Justice and Interior Ministers of the Eight (1997), Communiqué
33. Principles on Trans-Border Access to Stored Computer Data (1999)
34. Principles on the Availability of Public Data Essential to Protecting Public Safety (2002)
35. Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations (2002)
36. Principles for Protecting Critical Information Infrastructure (2003)
37. Best Practices for Network Security, Incident Response and Reporting to Law Enforcement (2004)
38. Best Practices for Law Enforcement Interaction with Victim-Companies During a Cyber-Crime Investigation (2005)

International Telecommunication Union

39. Resolution on Non-Discriminatory Access and Use of Internet Resources (2008)
40. Sample Legislative Language for Cyber Crime

Organisation for Economic Co-Operation and Development

41. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), including the Annex to the Recommendation of the Council of 23rd September 1980 Guidelines governing the protection of privacy and transborder flows of personal data
42. Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security (2002)
43. BIAC and MAAWG Best Practices for Internet Service Providers and Network Operators Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003)
44. Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam (2006)
45. Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)

Organization for Security and Co-Operation in Europe

46. Ministerial Council Decision No. 3/04 "Combating the Use of the Internet for Terrorist Purposes" (2004)
47. OSCE Ministerial Council Decision No. 7/06 "Countering the Use of the Internet for Terrorist Purposes" (2006)
48. Parliamentary Assembly "Astana" Resolution on Cyber Security and Cyber Crime (2008)

United Nations

49. Guidelines for the regulation of computerised personal data files (Regulation 44/132 of 5 December 1989).

50. Guidelines for the regulation of computerised personal data tiles (Resolution 45/95 of 14 December 1990).
51. Developments in the field of information and telecommunications in the context of international security (Resolution 53/70 of 4 December 1998)
52. Developments in the field of information and telecommunications in the context of international security (Resolution 54/49 of 1 December 1999)
53. Developments in the field of information and telecommunications in the context of international security (Resolution 55/28 of 20 November 2000)
54. Combating the criminal misuse of information technologies (Resolution 55/63 of 4 December 2000)
55. Developments in the field of information and telecommunications in the context of international security (Resolution 56/19 of 29 November 2001)
56. Combating the criminal misuse of information technologies (Resolution 56/121 of 19 December 2001)
57. Developments in the field of information and telecommunications in the context of international security (Resolution 57/53 of 22 November 2002)
58. Creation of a global culture of cyber security (Resolution 57/239 of 20 December 2002)
59. Developments in the field of information and telecommunications in the context of international security (Resolution 58/32 of 8 December 2003)
60. Creation of a global culture of cyber security and the protection of critical information infrastructures (Resolution 58/199 of 23 December 2003)
61. Developments in the field of information and telecommunications in the context of international security (Resolution 59/61 of 3 December 2004)
62. Developments in the field of information and telecommunications in the context of international security (Resolution 60/45 of 8 December 2005)
63. Developments in the field of information and telecommunications in the context of international security (Resolution 61/54 of 6 December 2006)
64. Developments in the field of information and telecommunications in the context of international security (Resolution 62/17 of 5 December 2007)
65. Developments in the field of information and telecommunications in the context of international security (Resolution 63/37 of 2 December 2008)

Annex 3. Cyber Security Related ECJ Case Law

Case **72/83** Campus Oil Limited and others v Minister for Industry and Energy and others.

Case **C-70/94** Fritz Werner Industrie-Ausrüstungen GmbH v Federal Republic of Germany.

Case **T-174/95** Svenska Journalistförbundet v Council of the European Union

Case **C-369/98** The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher.

Joined Cases **C-465/00**, **C-138/01** and **C-139/01** Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk

Case **C-101/01** Criminal proceedings against Bodil Lindqvist

Case **C-243/01** Criminal proceedings against Piergiorgio Gambelli and Others

Case **C-71/02** Herbert Karner Industrie-Auktionen GmbH v Troostwijk GmbH

Case **T 253/02** Chafiq Ayadi v Council of the European Union

Case **C-176/03** Commission of the European Communities v Council of the European Union

Case **C-89/04** Mediakabel BV v Commissariaat voor de Media

Case **T-99/04** AC-Treuhand AG v Commission of the European Communities

Case **T-194/04** The Bavarian Lager Co. Ltd v Commission of the European Communities

Joined Cases **C-317/04** and **C-318/04** European Parliament v Council of the European Union and Commission of the European Communities

Case **T-362/04** Leonid Minin v Commission of the European Communities

Case **C-150/05** Jean Leon Van Straaten v Staat der Nederlanden and Republiek Italië

Case C-**306/05** Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA

Joined Cases **C-402/05 P** and **C-415/05 P** Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities

Case **C-467/05** Criminal proceedings against Giovanni Dell'Orto

Case **C-244/06** Dynamic Medien Vertriebs GmbH v Avides Media AG

Case **C-275/06** Productores de Música de España (Promusicae) v Telefónica de España SAU

Case **C-524/06** Heinz Huber v Bundesrepublik Deutschland

Case **C-73/07** Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy

Case **C-421/07** Criminal Proceedings against Frede Damgaard

Case **C-553/07** College van Burgemeester en Wethouders van Rotterdam v M.E.E. Rijkeboer

Case **C-553/07** College van Burgemeester en Wethouders van Rotterdam v M.E.E. Rijkeboer

Annex 4. Cyber Security Related ECHR Case Law

Case of Denisova and Moiseyeva v. Russia (Application no. 16903/03)
Case of Fatullayev v. Azerbaijan (Application no. 40984/07)
Case of Kennedy v. the United Kingdom (Application no. 26839/05)
Case of K.U. v. Finland (Application no. 2872/02)
Case of Times Newspapers LTD (Nos. 1 and 2) v. the United Kingdom (Application no. 3002/03 and 23676/03)
Case of Liberty and Others v. the United Kingdom (Application no. 58243/00)
Case of S. and Marper v. the United Kingdom (Application no. 30562/04 and 30566/04)
Case of Megadat.com SRL v. Moldova (Application no. 21151/04)
Case of Ramanauskas v. Lithuania (Application no. 74420/01)
Case of Wieser and Bicos Beteiligungen GmbH v. Austria (Application no. 74336/01)
Case of Copland v. the United Kingdom (Application no. 62617/00)
Case of Smirnov v. Russia (Application no. 71362/01)
Case of Petri Sallinen and Others v. Finland (Application no. 50882/99)
Case of Malone v. the United Kingdom (Application no. 8691/79)
Case of Bykov v. Russia (Application no. 4378/02)
Case of Iordachi and Others v. Moldova (Application no. 25198/02)
Case of Kvasnica v. Slovakia (Application no. 72094701)
Case of Volokhy v. Ukraine (Application no. 23543/02)
Case of Taylor-Sabori v. the United Kingdom (Application no. 47114/99)
Case of Amann v. Switzerland (Application no. 27798/95)
Case of Kopp v. Switzerland (Application no. 13/1997/797/1000)
Case of Lambert v. France (Application no. 88/1997/872/1084)
Case of Valenzuela Contreras v. Spain (Application no. 58/1997/842/1048)
Case of Autronic ag v. Switzerland (Application no. 12726/87)
Case of Huvig v. France (Application no. 11105/84)
Case of Kruslin v. France (Application no. 11801/85)
Case of Klass and Others v. Germany (Application no. 5029/71)
Case of Guja v. Moldova (Application no. 14277/04)
Case of Satik v. Turkey (No. 2) (Application no. 60999/00)
Case of Stoll v. Switzerland (Application no. 69698/01)
Case of Segerstedt-Wiberg and Others v. Sweden (Application no. 62332/00)
Case of Pasko v. Russia (Application no. 69519/01)
Case of Dowsett v. the United Kingdom (Application no. 39482/98)
Case of Özgür Gündem v. Turkey (Application no. 23144/93)
Case of Gerger v. Turkey (Application no. 24919/94)
Case of Zana v. Turkey (Application no. 69/1996/688/880)
Case of A. and Others v. the United Kingdom (Application no. 3455/05)
Case of Nuray Şen v. Turkey (Application no. 41478/98)
Case of Brannigan and McBride v. the United Kingdom (Application no. 14553/89, 14554/89)
Case of Lawless v. Ireland (No. 3) (Application no. 332/57)
Case of Vajnai v. Hungary (Application no. 33629/06)
Case of Ždanoka v. Latvia (Application no. 58278/00)

CURRICULUM VITAE

General Data

Name:	Eneken Tikk (Ms.)
Date of birth:	August 22, 1976
Place of birth:	Tartu, Estonia
Contacts:	+372 507 2270, eneken.tikk@ccdcoe.org

Education

2004–	*Stud. Dr. Iur.,* Tartu University (Estonia), Faculty of Law, areas of interest: Information Technology and Cyber Defense law
2009–2010	U.S. National Defense University Chief Information Assurance Officer Course
Oct 2005	Visiting Student, Freiburg University (Germany), Seminar on Personal Data Protection supervised by Prof. F. Schoch
2000–2004	*Magister Juris*, University of Tartu, Faculty of Law, areas of interest: IT and Electronic Communications law
Jan–Apr 2004	Long-Term Attending Student, Stockholm University (Sweden), Department of Law, LL.M Program on EU Intellectual Property Law
Aug–Dec 2003	Long-Term Attending Student, Stockholm University, Department of Law, IT & Law LL.M Program,
Mar–Apr 2003	Visiting Student, Helsinki University (Finland)
1994–1998	*Baccalaureus Artium*, (Law), University of Tartu, Faculty of Law, areas of interest: public international law and law of armed conflicts, human rights
1994	German Class graduate, Tartu Raatuse Gymnasium

Professional / consulting experience

2009	George Mason University, Research Fellow at the Center for Infrastructure Protection in the School of Law
2007–2009	Cooperative Cyber Defence Centre of Excellence (CCD COE) Legal Advisor
2008–2009	Head of the Legal Task Team
2010	acting Legal and Policy Branch Chief
2007–2008	Estonian Ministry of Defense, Head of the Cyber Defence Legal Expert Team
2008–2009, 2010–2013	Estonian Statistics Board, legal consultant for National Census Law reform
2007	Estonian Ministry of Justice, adviser on information law and legal policy

2006–2007 Estonian Defense Forces, Scientist (Cyber Defence Law)
2006 Estonian Ministry of Social Affairs, expert on E-Health Information System (data protection law)
2007–2009 Estonian Informatics Centre, legal expert on personal data, databases and public information law
2004–2006 LEXTAL Law Firm attorney
2003–2004 Law Firm Teder & Partnerid lawyer
2000–2004 DLL Ltd. lawyer and partner
2005–2006 Contract-based consulting for the Estonian Data Protection Inspectorate and the Estonian Chancellor of Justice and several Estonian private sector companies.

Teaching

since 2010 Swedish National Defense College, legal modules of the Chief Information Assurance Officer Course
2008, 2009 Tallinn Technical University, cyber defense legal framework for IT students
since 2006 Tartu University, lecturer on information law and legislative drafting
since 2004 Estonian Business School, lecturer, courses on IT and E-Commerce Law
2004–2007 Estonian Academy of State Defence, lecturer on Information law and public information systems
1998–2002 Estonian Military Academy, lecturer on state defense law, public international law and human rights law
Estonian E-Governance Academy, lecturer on IT law and legal policy

Fieldwork and participation in R&D programs

2007–2008 NATO Cyber Defence Task Force, Legal Aspects of NATO Cyber Defence Concept
2005–2009 Tartu University/Estonian Science Foundation, Harmonization of Information Law and Legal Theoretical Approach to Regulation of Information
2007–2011 Tartu University/Estonian Science Foundation, Estonian Legal Space in Global Legal Space
2007 Estonian Ministry of Economy and Communications, Legal Expert Group on Cyber Defense
2007 Estonian Ministry of Defense, Joint Analysis Group on Cyber Defense and National Cyber Strategy
2007 Estonian Ministry of Justice, leading preparations for 2nd Data Protection Evaluation for Schengen Information System

2006	Estonian Ministry of Social Affairs, Legal Expert to the E-Health Information System
2002	UNESCO ICII Conference, Delegate of UNESCO ENC, Mainz
2005	Leiden
2002	Joint Seminar of Kiel and Lund Universities "Unification of International and EU Law in the Field of IT"

Professional association

- Estonian IT Law Association, founder
- Estonian E-Business Society, chairman
- DLL IT and Media Law Institute, founder, chairman
- Estonian Bar Association, member (membership suspended due to public service)
- International Law Association, Estonian Branch, member
- Estonian Information Technology Society, member
- Law Philosophy Society of Estonia, member

Language competences 1…5
Estonian (mother tonque), English (4), German (3+), Russian (3+)

Professional papers and articles

Books

1. **Ants Nõmper, Eneken Tikk**. Information and Law. Juura, Õigusteabe AS 2007. (Textbook on legal regulation of use of information, data protection, data privacy etc.)
2. **Eneken Tikk, Kadri Kaska, Liis Vihul**. International Cyber Incidents: Legal Considerations, CCD COE 2010
3. **Eneken Tikk**. Frameworks for International Cyber Security: Legal and Policy Instruments. CCD COE Publishing, 2010.
4. **Eneken Tikk**. Frameworks for International Cyber Security: Case Law. CCD COE Publishing, 2010.
5. **Eneken Tikk**. Frameworks for International Cyber Security: National Cyber Security Strategies. CCD COE Publishing, 2011
6. **Eneken Tikk, Anna-Maria Talihärm** (Editors). International Cyber Security Legal and Policy Proceedings. CCD COE Publishing, 2010.

Articles

7. **Eneken Tikk**. Internet and Law, Juridica, 2000, No.6, pages 402–407.
8. **Eneken Tikk**. Internet Service Provider's Liability. Arvutimaailm (2000) No. 5

9. **Eneken Tikk**. Legal Restrictions to the Choice of a Domian Name. Arvutimaailm (2000) No. 6
10. **Eneken Tikk**. Web Design Agreements. Arvutimaailm (2001) No. 1
11. **Eneken Tikk**. Legal Framework of E-Commerce. Arvutimaailm (2001) No. 2
12. **Eneken Tikk**. Advertising in the Internet. Arvutimaailm (2001) No. 3
13. **Eneken Tikk**. Privacy on the Internet – why and how? Arvutimaailm (2001) No. 5
14. **Eneken Tikk**. Digital Media Victims – Copyright on the Internet. Arvutimaailm (2001) No. 7
15. **Eneken Tikk**. Influence of Terrorism on Cyberlaw. Arvutimaailm (2001) No. 9
16. **Eneken Tikk**. Cookies – Pro and Contra. Arvutimaailm (2002) No. 1
17. **Eneken Tikk**. Whose Rules Apply in Cyberspace? Arvutimaailm (2002) No. 2, 3, 4
18. **Eneken Tikk**. New Trends in Internet Service Provider's Liability – Also for Estonia? Arvutimaailm (2002) No. 5
19. **Eneken Tikk**. Software Piracy Fight in Estonia. Arvutimaailm (2002) No. 6
20. **Eneken Tikk**. Protecting Privacy in the Knowledge Society. Arvutimaailm (2002) No. 7
21. **Eneken Tikk**. IT Contracting. Arvutimaailm (2002) No. 8
22. **Eneken Tikk**. Protecting Authors' Rights on the Internet. Arvutimaailm (2002) No. 9–10
23. **Eneken Tikk**. Aja ja ruumi õiguslik kontseptsioon teadmiste ühiskonna õiguse keskse probleemina, Juridica, 2002, No.9, pages.579–585
24. **Eneken Tikk**. Implementation of the Estonian Public Information Act. Arvutimaailm (2003) No. 1
25. **Eneken Tikk**. Is Digital Word Free? Arvutimaailm (2003) No. 2
26. **Eneken Tikk**. Thoughts on Freedom of Information. Arvutimaailm (2003) No. 3
27. **Eneken Tikk**. Between Yesterday and Tomorrow. Arvutimaailm (2003) No. 4
28. **Eneken Tikk**. The Beauty and Pain of Surveillance. Arvutimaailm (2003) No. 5
29. **Eneken Tikk**. Consumer Rights in E-Commerce. Arvutimaailm (2003) No. 6
30. **Eneken Tikk**. Using Your Office Computer – Legal Perspective. Arvutimaailm (2003) No. 7
31. **Eneken Tikk**. Know Your ICT Staff. Arvutimaailm (2003) No. 9
32. **Eneken Tikk**. What's the Use of a Disclaimer? Arvutimaailm (2003) No. 10
33. **Eneken Tikk**. Identity Theft. Arvutimaailm (2004) No. 1
34. **Eneken Tikk**. Official Data on the Internet. Arvutimaailm (2004) No. 3
35. **Eneken Tikk**. Critique to the Information Society Services Act. Arvutimaailm (2004) No. 4

36. **Eneken Tikk**. Protecting Databases in the EU. Arvutimaailm (2004) No. 5
37. **Eneken Tikk, Tõnu Runnel**. ICT Risks Can Destroy Your Business. Arvutimaailm (2004) No. 6
38. **Eneken Tikk**. New Law on the Secrecy of Communications. Arvutimaailm (2004) No. 7
39. **Eneken Tikk**. Legal Aspects of Biometrics. Arvutimaailm (2004) No. 8
40. **Eneken Tikk**. Website Owners Ignore Legal Requirements. Arvutimaailm (2004) No. 9
41. **Eneken Tikk**. Traffic Data – Not Only from the Traffic Authority. Arvutimaailm (2004) No. 10
42. **Eneken Tikk**. Spam – Everybody Help Yourself. Arvutimaailm (2005) No. 1
43. **Eneken Tikk**. End-User Rights. Arvutimaailm (2005) No. 2
44. **Eneken Tikk**. Software Development Sub-Contracting. Arvutimaailm (2005) No. 3
45. **Eneken Tikk**. Protecting Childrens' Rights in the Information Society. Arvutimaailm (2005) No. 4
46. **Eneken Tikk**. Web Advertisement Subject to Legal Restrictions. Arvutimaailm (2005) No. 6
47. **Eneken Tikk, Monika Mikiver.** (2005). Informatsioonilise enesemääramise õiguse tagamise diskretsiooniotsused haldusmenetluses. Juridica, IV, 250–258.
48. **Eneken Tikk**. Deep Linking. Arvutimaailm (2005) No. 7
49. **Eneken Tikk, Monika Mikiver**. (2006). Applicability of the Census Case in Estonian Personal Data Protection Law. Juridica International, 1, 102–110.
50. **Eneken Tikk**. Information and Law. Õiguskeel (2007) nr 4.
51. **Eneken Tikk, Reet Oorn.** "Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism" NATO Science for Peace and Security Series – E: Human and Societal Dynamics, vol. 34, 2008 (Responses to Cyber Terrorism). Edited by the Centre of Excellence Defence Against Terrorism, Ankara, Turkey
52. **Eneken Tikk**. "Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective" NATO Science for Peace and Security Series – E: Human and Societal Dynamics, vol. 59, 2009 (Modelling Cyber Security: Approaches, Methodology, Strategies). Edited by Umberto Gori
53. **Eneken Tikk, Kadri Kaska**. Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons (Proceedings of the 9th European Conference on Information Warfare and Security Hosted by Strategy-international.org and the Department of Applied Informatics University of Macedonia Thessaloniki, Greece 1–2 July 2010). Edited by Josef Demergis)
54. **Eneken Tikk**. Global Cyber Security – Thinking About Ways Ahead for NATO, SAIS Review – Volume 30, Number 2, Summer-Fall 2010, pp. 105–119

55. **James Bret Michael, Eneken Tikk, Peter Wahlgren, Thomas C. Wingfield.** "From Chaos to Collective Defense" Computer, vol. 43, no. 8, pp. 91–94, Aug. 2010, (Security, Conflict, Deterrence, Arms Control, Law, Policy)

Frequent contributions to Estonian daily newspapers and IT related publications.

ELULOOKIRJELDUS

Nimi:	Eneken Tikk
Sünniaeg:	22. 08. 1976
Sünnikoht:	Tartu, Eesti
Kontakt:	+372 50 722 70
Kontaktaadress:	Aasa 13, Peetri küla, Rae vald, Harjumaa 75301 et@dll.ee (e-post)

Hariduskäik

alates 2004	Tartu Ülikool, doktoriõpe, (infoühiskonna- ja IT-õigus)
2004–2005	Stockholmi Ülikool, magistriprogramm Euroopa Liidu Intellektuaalomandi õiguses,
2003–2004	Stockholmi Ülikool, magistriprogramm IT ja intellektuaalomandi õiguses,
2005	Freiburgi Ülikool, seminar andmekaitseõigusest,
2003	Helsinki Ülikool, vahetusüliõpilane,
2000–2004	*Magister iuris,* Tartu Ülikool, IT- ja kommunikatsiooniõigus, privaatsusõigused ja andmekaitse ning inimõiguste realiseerumine eraõiguses
1994–1998	BA (õigusteadus), Tartu Ülikool, Rahvusvaheline avalik õigus, EL õigus, inimõigused, juriidiline inglise keel
1994	Saksa keele süvaõppeklass, Tartu Raatuse Gümnaasium

Erialane töökogemus

2009	George Mason'i Ülikooli õigusteaduskond (USA), uurimisstipendiaat
alates 2006	Kooperatiivse Küberkaitse Kompetentsikeskuse õigusnõunik, õigus- ja poliitikaosakonna juhataja
2007	Riigi Infosüsteemide Arenduskeskus, õigusekspert
2007	Kaitseministeerium, küberjulgeoleku strateegia õigusekspertide töörühma juht
2007–2008	Justiitsministeerium, andmekaitse nõunik
alates 2006	Andmekaitse Inspektsioon, nõunik
alates 2004	Advokaadibüroo Lextal, advokaat
2000–2004	DLL OÜ, jurist

Õppetöö läbiviimise kogemus

alates 2010 Rootsi Kaitseülikool, Infoturbe kursuse õigusained,
2005 Tartu Ülikool, õigusloome alused, informatsioon ja õigus,
2007–2009 Tallinna Tehnikaülikool, küberjulgeoleku õiguslikud alused,
2004–2007 Sisekaitseakadeemia, teabeõiguse lektor,
2003 Eesti Õiguskeskus, kohtunike koolituse programm,
2002 Eesti Infotehnoloogia Selts, IT-õiguse alane koolitus.
2001–2006 Estonian Business School, IT- ja E-kaubanduse õigus,

Erialane liikmelisus

– Rahvusvahelise Õiguse Assotsiatsioon (*International Law Association*), Eesti haru, liige
– EBS Teadmiste Ühiskonna Seminar, liige
– Eesti Advokatuur, vandeadvokaadi vanemabi (liikmesus peatatud seoses avaliku teenistusega)

Keeled
Eesti, inglise, saksa, vene

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS

1. **Херберт Линдмяэ.** Управление проведением судебных экспертиз и его эффективность в уголовном судопроизводстве. Тарту, 1991.
2. **Peep Pruks.** Strafprozesse: Wissenschaftliche “Lügendetektion”. (Instrumentaldiagnostik der emotionalen Spannung und ihre Anwendungsmöglichkeiten in Strafprozess). Tartu, 1991.
3 **Marju Luts.** Juhuslik ja isamaaline: F. G. v. Bunge provintsiaalõigusteadus. Tartu, 2000.
4. **Gaabriel Tavits.** Tööõiguse rakendusala määratlemine töötaja, tööandja ja töölepingu mõistete abil. Tartu, 2001.
5. **Merle Muda.** Töötajate õiguste kaitse tööandja tegevuse ümberkorraldamisel. Tartu, 2001.
6. **Margus Kingisepp.** Kahjuhüvitis postmodernses deliktiõiguses. Tartu, 2002.
7. **Vallo Olle.** Kohaliku omavalitsuse teostamine vahetu demokraatia vormis: kohalik rahvaalgatus ja rahvahääletus. Tartu, 2002.
8. **Irene Kull.** Hea usu põhimõte kaasaegses lepinguõiguses. Tartu, 2002.
9. **Jüri Saar.** Õigusvastane käitumine alaealisena ja kriminaalsed karjäärid (Eesti 1985–1999 longituuduurimuse andmetel). Tartu, 2003.
10. **Julia Laffranque.** Kohtuniku eriarvamus. Selle võimalikkus ja vajalikkus Eesti Vabariigi Riigikohtus ja Euroopa Kohtus. Tartu, 2003.
11. **Hannes Veinla.** Ettevaatusprintsiip keskkonnaõiguses. Tartu, 2004.
12. **Kalev Saare.** Eraõigusliku juriidilise isiku õigussubjektsuse piiritlemine. Tartu, 2004.
13. **Meris Sillaots.** Kokkuleppemenetlus kriminaalmenetluses. Tartu, 2004.
14. **Mario Rosentau.** Õiguse olemus: sotsiaalse käitumise funktsionaalne programm. Tartu, 2004.
15. **Ants Nõmper.** Open consent – a new form of informed consent for population genetic databases. Tartu, 2005.
16. **Janno Lahe.** Süü deliktiõiguses. Tartu, 2005.
17. **Priit Pikamäe.** Tahtluse struktuur. Tahtlus kui koosseisupäraste asjaolude teadmine. Tartu, 2006.
18. **Ivo Pilving.** Haldusakti siduvus. Uurimus kehtiva haldusakti õiguslikust tähendusest rõhuasetusega avalik-õiguslikel lubadel. Tartu, 2006.
19. **Karin Sein.** Ettenähtavus ja rikutud kohustuse eesmärk kui lepingulise kahjuhüvitise piiramise alused. Tartu, 2007.
20. **Mart Susi.** Õigus tõhusale menetlusele enda kaitseks – Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsiooni artikkel 13 Euroopa Inimõiguste Kohtu dünaamilises käsitluses. Tartu, 2008.
21. **Carri Ginter.** Application of principles of European Law in the supreme court of Estonia. Tartu, 2008.
22. **Villu Kõve.** Varaliste tehingute süsteem Eestis. Tartu, 2009.

23. **Katri Paas.** Implications of Smallness of an Economy on Merger Control. Tartu, 2009.
24. **Anneli Alekand.** Proportsionaalsuse printsiip põhiõiguste riive mõõdupuuna täitemenetluses. Tartu, 2009.
25. **Aleksei Kelli.** Developments of the Estonian Intellectual Property System to Meet the Challenges of the Knowledge-based Economy. Tartu, 2009.
26. **Merike Ristikivi**. Latin terms in the Estonian legal language: form, meaning and influences. Tartu, 2009.
27. **Mari Ann Simovart.** Lepinguvabaduse piirid riigihankes: Euroopa Liidu hankeõiguse mõju Eesti eraõigusele. Tartu, 2010.
28. **Priidu Pärna.** Korteriomanike ühisus: piiritlemine, õigusvõime, vastutus**.** Tartu, 2010.
29. **René Värk.** Riikide enesekaitse ja kollektiivse julgeolekusüsteemi võimalikkusest mitteriiklike terroristlike rühmituste kontekstis. Tartu, 2011.
30. **Paavo Randma.** Organisatsiooniline teovalitsemine – *täideviija täideviija taga* kontseptsioon teoorias ja selle rakendamine praktikas. Tartu, 2011.
31. **Urmas Volens.** Usaldusvastutus kui iseseisev vastutussüsteem ja selle avaldumisvormid. Tartu, 2011.
32. **Margit Vutt.** Aktsionäri derivatiivnõue kui õiguskaitsevahend ja ühingujuhtimise abinõu. Tartu, 2011.
33. **Hesi Siimets-Gross.** Das „Liv-, Est- und Curlaendische Privatrecht" (1864/65) und das römische Recht im Baltikum. Tartu, 2011.
34. **Andres Vutt.** Legal capital rules as a measure for creditor and shareholder protection. Tartu, 2011.