



NORDREGIO
Nordic Centre for Spatial Development

Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection

**Christer Pursiainen (ed.) with the assistance of
Patrick Lindblom and Per Francke**

NORDREGIO REPORT 2007:5



Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection

Christer Pursiainen (ed.)
with the assistance of
Patrick Lindblom and Per Francke

NORDREGIO 2007

Nordregio Report 2007:5
ISSN 1403-2503
ISBN 978-91-89332-66-9

Nordregio
P.O. Box 1658
SE-111 86 Stockholm, Sweden
nordregio@nordregio.se
www.nordregio.se
www.norden.se

Cover design: Hanna Dobois
Cover photograph: Odd Iglebaek
Dtp: Patrick Lindblom
Linguistic editing: Mark Waller
Repro and print: Allduplo Offsettryck AB, Stockholm, Sweden

© Nordregio, the authors and the project.

This study has been part-financed by the European Commission Directorate-General Justice, Freedom and Security, European Programme for Critical Infrastructure Protection. The Commission is not responsible for any use that may be made of the information and analysis contained herein.

Nordic co-operation

takes place among the countries of Denmark, Finland, Iceland, Norway and Sweden, as well as the autonomous territories of the Faroe Islands, Greenland and Åland.

The Nordic Council

is a forum for co-operation between the Nordic parliaments and governments. The Council consists of 87 parliamentarians from the Nordic countries. The Nordic Council takes policy initiatives and monitors Nordic co-operation. Founded in 1952.

The Nordic Council of Ministers

is a forum of co-operation between the Nordic governments. The Nordic Council of Ministers implements Nordic co-operation. The prime ministers have the overall responsibility. Its activities are co-ordinated by the Nordic ministers for co-operation, the Nordic Committee for co-operation and portfolio ministers. Founded in 1971.

Stockholm, Sweden
2007

CONTENTS

LIST OF FIGURES, TABLES AND FACT BOXES.....	V
PREFACE	IX
ABOUT THE CONTRIBUTORS.....	XIII
EXECUTIVE SUMMARY	XV
LIST OF ACRONYMS	XXIX
CHAPTER I: INTRODUCTION	1
1 CRITICAL INFRASTRUCTURE PROTECTION IN THE BALTIC SEA REGION	3
1.1 <i>The European Programme for Critical Infrastructure Protection.....</i>	3
1.2 <i>The heterogenic Baltic Sea Region</i>	6
1.3 <i>What are critical infrastuctures?</i>	14
1.4 <i>Protection – against what?</i>	26
1.5 <i>From protection to resilience?</i>	31
1.6 <i>Dependencies and interdependencies.....</i>	33
1.7 <i>The dilemma of public-private partnership</i>	35
1.8 <i>EU and Member States – finding the right balance</i>	39
1.9 <i>Regional multilateralism in critical infrastructure protection.....</i>	45
1.10 <i>Conclusions</i>	53
CHAPTER II: ELECTRICITY.....	55
2 ELECTRIC POWER SYSTEMS BLACKOUTS AND THE RESCUE SERVICES: THE CASE OF FINLAND	57
2.1 <i>Introduction</i>	57
2.2 <i>The electric power systems</i>	58
2.3 <i>Electric power system disturbances</i>	66
2.4 <i>Better preparedness</i>	76
CHAPTER III: INFORMATION AND COMMUNICATION TECHNOLOGY	83
3 CRITICAL INFORMATION INFRASTRUCTURE PROTECTION IN THE BALTIC SEA REGION: THE CASE OF TETRA.....	85
3.1 <i>Problem description and definition.....</i>	85
3.2 <i>Case study on CIIP</i>	101
3.3 <i>Comprehensive strategy for CIIP.....</i>	124
3.4 <i>Conclusions and way forward.....</i>	137
CHAPTER IV: OIL TRANSPORTATION AND MARITIME SAFETY	141
4 RISKS IN OIL TRANSPORTATION IN THE GULF OF FINLAND. “NOT A QUESTION OF IF – BUT WHEN”	143
4.1 <i>Introduction</i>	143
4.2 <i>Oil transportation in the Gulf of Finland</i>	144
4.3 <i>Risk evaluation</i>	150
4.4 <i>Present safety solutions</i>	156
4.5 <i>Conclusions</i>	161
CHAPTER V: GAS	165
5 NORTH EUROPEAN GAS PIPELINE	167
5.1 <i>Introduction</i>	167
5.2 <i>The North European Gas Pipeline</i>	167
5.3 <i>Threat scenarios</i>	173

5.4	<i>Impacts caused by terrorism, natural disasters and dumped munitions.....</i>	178
5.5	<i>Critical infrastructure protection strategy</i>	182
CHAPTER VI: WATER		187
6	POTENTIAL RISKS FOR SHALLOW GROUNDWATER AQUIFERS IN COASTAL AREAS OF THE BALTIC SEA: A CASE STUDY IN THE HANKO AREA IN SOUTH FINLAND	189
6.1	<i>Introduction.....</i>	189
6.2	<i>Methodology and materials</i>	197
6.3	<i>Hanko aquifer.....</i>	198
6.4	<i>Risk assessment in the Hanko area</i>	204
6.5	<i>Risk management in the Hanko area</i>	209
6.6	<i>Adaptation of groundwater protection strategy in Hanko and other coastal aquifers in Finland</i>	211
6.7	<i>Conclusion.....</i>	213
BIBLIOGRAPHY		215

LIST OF FIGURES, TABLES AND FACT BOXES

FIGURE I—1	THE BALTIC SEA REGION	6
FIGURE I—2	POPULATION DENSITY IN THE BSR	8
FIGURE I—3	CITY POPULATION IN THE BSR	9
FIGURE I—4	GDP (PPS) PER CAPITA 2004 IN EUROPE.....	10
FIGURE I—5	DOMINANT BRANCH OF EMPLOYMENT IN THE BSR	11
FIGURE I—6	RELATIVE IMPORTANCE OF EUROPEAN STOCK EXCHANGES	12
FIGURE I—7	THE NORWEGIAN METHOD OF DEFINING CRITICALITY	25
FIGURE II—1	ELECTRICITY SUPPLY IN FINLAND YEAR 2006.....	59
FIGURE II—2	THE PEAK LOAD TREND	61
FIGURE II—3	THE ELECTRICITY TRANSMISSION GRID IN THE BSR.....	63
FIGURE II—4	STATE OF POWER SYSTEM	64
FIGURE II—5	MEASURES TAKEN BY RESCUE SERVICES	70
FIGURE II—6	THE CIVIL PROTECTION INFRASTRUCTURE AND THE POWER SUPPLY NETWORK AFFECTED	72
FIGURE II—7	THE CIVIL PROTECTION AND RADIO COMMUNICATION AFFECTED	73
FIGURE II—8	CUSTOMERS WITHOUT ELECTRICITY IN CLASS I MAJOR STORM.....	77
FIGURE II—9	CUSTOMERS WITHOUT ELECTRICITY IN CLASS II MAJOR STORM	78
FIGURE II—10	CUSTOMERS WITHOUT ELECTRICITY IN CLASS III MAJOR STORM	79
FIGURE III—1	SECTORS WHOSE OPERATIONS ARE STRONGLY DEPENDENT ON ICT	85
FIGURE III—2	RELATIONSHIP BETWEEN VARIOUS THREAT-RELATED CONCEPTS	87
FIGURE III—3	HIGH-LEVEL CONCEPT MAP DEPICTING VARIOUS ASPECTS OF THREATS ON CII	88
FIGURE III—4	A LOW-LEVEL CONCEPT MAPPING OF THE CONSEQUENCES OF REALIZED THREATS	90
FIGURE III—5	A LOW-LEVEL CONCEPT MAPPING OF THE POSSIBLE NATURE OF THREATS	91
FIGURE III—6	EXAMPLE OF TYPE OF AUTHORIZED ACCESS ACCORDED TO DIFFERENT GROUPS	93
FIGURE III—7	CONCEPT MAPPING OF MALICIOUS LOGIC IN INFORMATION AND COMMUNICATION SYSTEMS	97
FIGURE III—8	CERT-FI REPORTED INCIDENTS BETWEEN IN THE PERIOD BETWEEN 2002 AND 2007	100
FIGURE III—9	ILLUSTRATION OF THE DIVERSE ICT LANDSCAPE.....	101
FIGURE III—10	HANDHELD AND VEHICLE-MOUNTED TETRA MOBILE STATIONS	104
FIGURE III—11	EXAMPLE ARCHITECTURE OF A TETRA NETWORK	105
FIGURE III—12	BASIC CONFIGURATION OF VARIOUS TETRA AIR INTERFACES	107
FIGURE III—13	TYPICAL SERVICES FOR TETRA USERS. AN EXAMPLE SCREENSHOT OF A SHORT DATA SERVICE MESSAGE IS SHOWN INSET	108
FIGURE III—14	THREE CALL TYPES SUPPORTED IN TETRA NETWORKS	109
FIGURE III—15	POSITIONING OF VIRVE TETRA INFRASTRUCTURE AND THE BREAKDOWN OF VIRVE USER GROUPS	109
FIGURE III—16	ITU-T X.805 SECURITY ARCHITECTURE FOR END-TO-END NETWORK SECURITY.	111
FIGURE III—17	NINE UNIQUE PERSPECTIVES OR MODULES OF THE ITU-T X.805 SECURITY ARCHITECTURE	113
FIGURE III—18	BASIC STEPS TAKEN IN ENCRYPTED COMMUNICATIONS	114
FIGURE III—19	IMPLEMENTATION REGIONS FOR AIR INTERFACE AND END-TO-END ENCRYPTION SCHEMES	115
FIGURE III—20	POSSIBLE TETRA NETWORK SURVIVABILITY MECHANISMS BASED ON BASE STATION FALLBACK MODE, DMO AND MULTIHOMED CELLULAR NETWORK ARRANGEMENT	116

FIGURE III—21	EXAMPLE RECOVERY OF THE LINK BETWEEN MSC 3 AND GMSC USING A RESILIENT FOUR NODE SDH RING TOPOLOGY	117
FIGURE III—22	TETRA SYSTEM PERFORMANCE UNDER VARIOUS OPERATING CONDITIONS	122
FIGURE III—23	AVAILABLE BASE STATIONS UNDER NORMAL AND CRISIS CONDITIONS	123
FIGURE III—24	TETRA SYSTEM PERFORMANCE UNDER CRISIS MANAGEMENT IN VARIOUS LEVELS OF INFRASTRUCTURE DISRUPTION	123
FIGURE III—25	CONTINUOUS LIFECYCLE OF STRATEGY ON CIIP	124
FIGURE III—26	A HOLISTIC APPROACH TO CIIP POLICY MAKING	125
FIGURE III—27	FOUR NODE ORGANIZATION MODEL AND ITS INTRADEPENDENCIES.....	128
FIGURE III—28	ORGANIZATIONAL INTERDEPENDENCIES THAT MAY EXIST AT NATIONAL, REGIONAL AND INTERNATIONAL LEVELS	129
FIGURE III—29	SECURITY INVESTMENT GAP FOR CIIP OBSERVED UNDER THE VULNERABILITY BASED APPROACH	132
FIGURE IV—1	SEABED DEPTH IN THE GULF OF FINLAND	145
FIGURE IV—2	OIL TRANSPORTATION IN THE GULF OF FINLAND THROUGH MAJOR OIL-TERMINAL PORTS 1995-2005 AND ESTIMATED DEVELOPMENT TO YEAR 2015.....	146
FIGURE IV—3	TRAFFIC THROUGH THE MAJOR PORTS IN THE GULF OF FINLAND 2006.....	147
FIGURE IV—4	NUMBER OF PASSENGERS TRAVELLING THROUGH THE PORTS OF HELSINKI AND TALLINN	147
FIGURE IV—5	MARITIME TRAFFIC THROUGH THE ENTRANCE TO THE GULF OF FINLAND 2006.....	148
FIGURE IV—6	MARITIME TRAFFIC THROUGH THE ENTRANCE TO RUSSIA'S BALTIC PORTS 2006.....	149
FIGURE IV—7	WINTER ICE COVERAGE IN THE GULF OF FINLAND 1997-2006.....	152
FIGURE IV—8	ACCIDENTS BY TYPE IN THE GULF OF FINLAND 2000-2006.....	153
FIGURE IV—9	MARITIME TRAFFIC AND ACCIDENTS IN THE GULF OF FINLAND 2000-2006.....	154
FIGURE IV—10	GOFREP AREA AND TERRITORIAL WATERS	157
FIGURE V—1	TEN-E PRIORITY AXES.....	168
FIGURE V—2	PROJECTION OF GAS DEMAND IN THE EU	169
FIGURE V—3	MILESTONES FOR THE NEGP-PROJECT.....	170
FIGURE V—4	ROUTE OF THE PIPELINE PROPOSED BY NORD STREAM	172
FIGURE V—5	DUMPED MUNITIONS IN THE BALTIC SEA	177
FIGURE VI—1	MAP OF QUATERNARY SAND AND GRAVEL DEPOSITS, THE MOST IMPORTANT SHALLOW GROUNDWATER RESOURCES IN FINLAND	191
FIGURE VI—2	AMOUNT OF WATER DISTRIBUTED BY PUBLIC WATER WORKS IN FINLAND DURING YEARS 1970 – 2001	193
FIGURE VI—3	MEAN TEMPERATURES FOR THE SUMMER SEASONS FOR 2001, 2050 AND 2099 AND THE DIFFERENCE 2099/2001	196
FIGURE VI—4	GROUNDWATER MONITORING TOOL INSTALLATION AT THE WELL HP0306	198
FIGURE VI—5	THE HANKO CASE STUDY AREA ON THE QUATERNARY DEPOSIT MAP	199
FIGURE VI—6	CONCEPTUAL GEOLOGICAL MODEL OF THE FIRST SALPAUSSELKÄ FORMATION IN THE HANKO MAIN GROUNDWATER AREA	200
FIGURE VI—7	GROUNDWATER THICKNESS IN HANKO MAIN GROUNDWATER AREA. THE THICKNESS OF GROUNDWATER REFLECTS THE SURFACE OF THE BEDROCK UNDER THE QUATERNARY DEPOSITS.....	200
FIGURE VI—8	GROUNDWATER LEVEL OF OBSERVATION WELL HP66 AND OF OBSERVATION WELL HP306, SEA LEVEL AND AIR PRESSURE DATA DURING 12.2 – 12.6.2007	203
FIGURE VI—9	MAP OF HANKO GROUNDWATER RISKS.....	205
FIGURE VI—10	A) GROUNDWATER FLOW PATTERNS AND THE ZONE OF DISPERSION IN A COASTAL AQUIFER, B) OVER PUMPING LOWERS GROUNDWATER LEVEL AND MAY LEAD TO SALTWATER INTRUSION	207
FIGURE VI—11	TOPOGRAPHY MAP OF HANKO MAIN GROUNDWATER AREA WITH A 2-METRE-CONTOUR.....	208
FIGURE VI—12	GROUNDWATER PROTECTION STRATEGY IN COAST AREA AQUIFER	212
TABLE I—1	BSR COUNTRIES AND THEIR PARTICIPATION IN THE EU AND NATO	14
TABLE I—2	CI/KR SECTORS IN THE UNITED STATES	16
TABLE I—3	CRITICAL INFRASTRUCTURE SECTORS ACCORDING TO THE EU.....	18

TABLE I—4	GERMANY’S CRITICAL INFRASTRUCTURE SECTORS.....	20
TABLE I—5	FINLAND’S VITAL FUNCTIONS TO SOCIETY.....	21
TABLE I—6	ESTONIA’S SECTORS OF VITAL IMPORTANCE.....	22
TABLE I—7	CRITICAL SOCIETAL FUNCTIONS IN SWEDEN	24
TABLE I—8	NORWAY’S CRITICAL INFRASTRUCTURES AND CRITICAL SOCIETAL FUNCTIONS	25
TABLE I—9	MAIN PERMANENT REGIONAL COUNCILS, INSTITUTIONS AND NETWORKS IN THE BSR	46
TABLE I—10	MEMBERSHIP/PARTICIPATION IN REGIONAL COUNCILS, INSTITUTIONS AND NETWORKS IN THE BSR	48
TABLE I—11	REGIONAL COUNCILS, INSTITUTIONS AND NETWORKS IN THE BSR FROM THE PERSPECTIVE OF THE EU DEFINITION OF THE CI SECTORS	52
TABLE II—1	ELECTRICITY CONSUMPTION IN FINLAND AND EUROPE	60
TABLE III—1	TWO ALTERNATIVE DEFINITIONS ON INFORMATION SECURITY, THREAT, ATTACK AND VULNERABILITY	86
TABLE III—2	AVERAGE INTENSITY CLASSIFICATION OF PAST OCCURRENCES OF NATURAL HAZARDS IN THE BSR.....	91
TABLE III—3	BRIEF OVERVIEW OF ACTIONS AND POSITIONING OF VARIOUS DELIBERATE CII THREAT ACTORS	94
TABLE III—4	BRIEF OVERVIEW OF ACTIONS AND POSITIONING OF VARIOUS NON-DELIBERATE CII THREAT ACTORS	96
TABLE III—5	EXISTING STATUS OF PSS TETRA NETWORK IMPLEMENTATIONS IN THE BSR AS OF EARLY 2007	103
TABLE III—6	COMPARISON OF KEY SYSTEM CHARACTERISTICS BETWEEN TETRA AND GSM	107
TABLE III—7	THREATS DEFINED IN ITU-T X.805 FRAMEWORK AND CORRESPONDING SECURITY DIMENSIONS PROPOSED TO ADDRESS THEM	113
TABLE III—8	SECURITY OBJECTIVES OF THE NINE UNIQUE MODULES OF THE ITU-T X.805 SECURITY ARCHITECTURE	114
TABLE III—9	SECURITY CLASSES DEFINED BY THE TETRA STANDARDS	115
TABLE III—10	TETRA NETWORK SECURITY MEASURES ADDRESSED IN MODULES 1-3 OF THE ITU-T X.805 SECURITY ARCHITECTURE.....	119
TABLE III—11	TETRA NETWORK SECURITY MEASURES ADDRESSED IN MODULES 4-6 OF THE ITU-T X.805 SECURITY ARCHITECTURE.....	120
TABLE III—12	TETRA NETWORK SECURITY MEASURES ADDRESSED IN MODULES 7-9 OF THE ITU-T X.805 SECURITY ARCHITECTURE.....	121
TABLE V—1	INTERSECTIONS OF NORD STREAM WITH EXCLUSIVE ECONOMIC ZONES AND TERRITORIAL WATERS IN THE BALTIC SEA.....	170
TABLE V—2	PULL-OUTS OF CHEMICAL MUNITIONS EAST OF BORNHOLM REGISTERED BY DENMARK	180
TABLE VI—1	COMPARISON OF GROUNDWATER QUALITY PARAMETERS IN THE HANKO PENINSULA TO FINNISH AVERAGE	202
FACT BOX IV—1	THE GULF OF FINLAND.....	145
FACT BOX V—1	BASIC AND TECHNICAL FACTS OF THE NEGP.....	171
FACT BOX V—2	PERMISSION PROCEDURE FOR NEGP IN GERMAN EEZ AND TW	174
FACT BOX V—3	EFFECTS OF A GAS LEAK ON THE NEGP	179

PREFACE

With the Commission Green Paper, published in November 2005, and Proposal for a Directive of the Council from December 2006, a European dimension has emerged in the field of critical infrastructure protection. The purpose of this study is to contribute to the European Programme for Critical Infrastructure Protection from the specific perspective of the Baltic Sea Region.

All countries have their own national traditions, institutional structures, policies and strategies, vocabulary, technical and methodological approaches and so forth as to how they protect their critical infrastructures or vital societal functions against different types of risks, threats and vulnerabilities.

The development towards a more integrated European critical infrastructure protection is a clear challenge for the national models and strategies, which differ from country to country. How would it be possible to combine the national and European levels of critical infrastructure protection into a harmonized and effective strategy?

Another challenge is the regional dimension. How, in the context of the EU-27, would it be possible to take into account the particular regional cross-border effects of critical infrastructure vulnerabilities as well as the specific features – such as particular weather conditions, technological capabilities, political and administrative systems, safety culture – of European sub-regions, such as the Baltic Sea Region?

This study aims at discussing these issues from several angles. While it draws a general picture of critical infrastructure protection in the region's context, it initiates discussion about the issue of whether a regional level of critical infrastructure protection would be needed as an intermediate level between the strategies of national governments and the European Union. This study also offers some detailed case studies, showing the complexity of the issues at stake. It provides information, arguments and proposals that hopefully will lead to even more vigorous debates and discussion on critical infrastructure protection in Europe and elsewhere and aims to contribute to much needed awareness-raising in this field.

This study is the result of a generous grant from the European Commission Directorate-General Justice, Freedom and Security. We owe special gratitude to the Commission for its kind support and smooth cooperation, which helped us to start a year-long cooperation between several partners.

The project started in December 2006 and was led by Dr. Christer Pursiainen from Nordregio – Nordic Centre for Spatial Development, a joint Nordic institute located in Stockholm, Sweden. Other contributing partners included University of Helsinki, Aleksanteri Institute (Finland), Emergency Services College (Finland), Geological Survey of Finland, Communications Laboratory of Helsinki University of Technology (Finland) and INFRASTRUKTUR & UMWELT, Professor Böhm und Partner (Germany). We have prepared the current study together with these partners.

Throughout the project the authors greatly benefited from the existence of a network of advisors from competent authorities and other stakeholders. This advisory network included the Swedish Emergency Management Agency, National Emergency Supply Agency (Finland), Ministry of Interior of Finland, Rescue Department, Ministry of Defense of Finland, The Main School of Fire Service (Poland) and EADS Secure Networks Oy (Finland). Our particular thanks go to these institutions for their fruitful cooperation and the professional, practice-oriented input to our study.

The project has also benefited from being part of a larger network, the CIVPRO Civil Protection Network, coordinated by Dr. Timo Hellenberg from the Aleksanteri Institute of the University of Helsinki. This network, which made the project possible in the first place, has also contributed to the current study by facilitating cooperation with, and learning processes from, a wide range of other related projects.

Within the framework of the project and CIVPRO, we organised in 2007 several smaller workshops and one larger conference on critical infrastructures. The International Conference on Critical Infrastructure Protection was held in the House of Estates in Helsinki 4-5 October, 2007. The conference was sponsored, beside the Commission, by the Finnish Prime Minister's Office and the United States Embassy to Finland (U.S. Department of State). Our particular thanks go to these institutions.

The conference provided the chance to exchange views with a wide range of high-level specialists and professionals from several countries and institutions, such as the European Commission, Finnish government and Prime Minister's Office, United States Department of Homeland Security, Swedish Emergency Management Agency, United Nations/International Strategy for Disaster Reduction, London Underground and several other authorities and research institutions. The presentations of the distinguished speakers are available at CIVPRO's website <http://www.helsinki.fi/aleksanteri/civpro>.

There are many people to acknowledge, who were generous with their time, support, assistance, professional information and comments, and presentations during the project. These people include Matti Aaltonen, William Anderson, Ole Arhenius, James Caverly, Aapo Cederberg, Ole Damsgaard, Charles Gadomski, Ivan Gotovchits, Rein Haavel, Axel Hagelstam, Timo Härkönen, Andrei Iatsenia, Ilkka Kananen, Timo Kinnunen, Markku Kivinen, Kari Kosonen, Richard Langlais, Mark Lewis, Jan Lundberg, Angelica Matveeva, Jukka Metso, Jens Müller, Radica NUSDORFER, Kimmo Paakkonen, Are Piel, Arto Pullinen, Hannu Rantanen, Reijo Salminen, René Sirol, Bengt Sundelius, Vladimir Vasilyev, Risto Volanen.

Any project, especially one financed by the EU, needs highly qualified administrative and financial professionals to carry out the complicated tasks related to budget management and financial reporting. We have been lucky to work with such people, especially Jacob Boëthius and Anita Kullén from Nordregio. Thanks also go to Sophie Didriksson, Brita Larsson and Liselott Happ-Tillberg from Nordregio as well as Essi Lindroos and Anne Pynnönen from the Aleksanteri Institute, for their help in organizing the seminars and conferences and for taking care of other practicalities. Mark Waller is particularly to be thanked for the quick and professional proof-reading and language editing of the manuscript.

The study includes tens of maps and other figures. *If not otherwise indicated*, the credit and copyright for these figures go as follows: In Chapter I, the general maps on the Baltic Sea Region have been prepared by Nordregio within several previous projects. In Chapter II, the maps on electricity networks have been prepared by Patrick Lindblom, Johanna Roto and Viktoria Barthofer from Nordregio for this project. The figures in Chapter III on information and communication technology have been prepared by the Communications Laboratory of Helsinki University of Technology. The maritime transport and safety maps in Chapter IV have been prepared by Patrick Lindblom and Viktoria Barthofer from Nordregio for this project. The maps and other figures in Chapter V, dealing with the North European Gas Pipeline, have been prepared by *Nord Stream*, and used with the company's permission. The maps and other figures in Chapter VI on ground water issues have been prepared or modified by the Geological Survey of Finland. We are also grateful to Odd Iglebaek, who has taken the photograph used in the cover.

Finally, the authors want to make it clear that all possible mistakes and misunderstandings, as well as interpretations, arguments, conclusions and policy recommendations contained herein remain however the *sole responsibility of the authors of the respective individual chapters*, including the Introduction. The Commission, the advisory network partners and other institutions and individual persons mentioned above are not responsible for any use that may be made of the information and analysis contained herein.

Stockholm, November 2007

ABOUT THE CONTRIBUTORS

Birgitta Backman is a Senior Scientist at the Geological Survey of Finland. She took her PhD degree in Geology at Helsinki University on the subject of groundwater quality, acidification, and recovery trends.

Viktoria Barthofer has a BSc degree in Urban and Regional planning and is a student in the Master's Programme in Regional Planning and Development at the Vienna University of Technology. She was a trainee at Nordregio in 2007.

Krisztina Cziner is Research Manager at Helsinki University of Technology leading the Public Safety Communications research group. She is a Doctor of Science in Technology.

Per Francke is a Researcher at Nordregio and has an MSc in Urban and Regional Planning with a Major in Human Geography, Stockholm University.

Sven Friedrich is Consultant at INFRASTRUKTUR & UMWELT, Potsdam. He holds a Diploma in Environmental Engineering from the Technical University of Cottbus, including one year of studies at the University Cracow.

Timo Hellenberg is the Liaison Head of the Aleksanteri Institute, at the University of Helsinki. He is a Doctor of Political Science and coordinates the CIVPRO Civil Protection Network.

Petter Holmström worked in 2007 as Project Planner at the Rescue Department in the State Provincial Office of Western Finland. He is a student in Åbo Akademi University Faculty of Technology.

Riikka Ikonen works as Project Manager at Culminatum Oy and was prior to that a Researcher at Nordregio. She has an MSc in Spatial Planning from the Royal Institute of Technology in Stockholm and a Bachelor of Administrative Sciences degree from the University of Tampere.

Risto Järvinen is a research assistant at the Helsinki University of Technology. He is an undergraduate student in the Communications Laboratory at the Helsinki University of Technology.

Jukka Laitinen has an MSc in Technology, focussing on economic geology, from the University of Helsinki. He is currently a geophysicist at the Geological Survey of Finland.

Jyrki Landstedt works as a Senior Officer at the Rescue Department in the State Provincial Office of Western Finland. He has an MSc in Engineering from Tampere University of Technology. He has long working experience from the various positions he has held in the Emergency Services sector in Finland.

Patrick Lindblom is a Researcher at Nordregio. He holds an MSc in Biology from Stockholm University, as well as a BA in Business Administration, also from Stockholm University.

Jan Lucenius is a Research scientist at the Helsinki University of Technology. He is a diploma engineer.

Samrit Luoma is a Scientist at the Geological Survey of Finland, specialized in groundwater studies. She has an MSc degree in Geology.

Edward Mutafulungwa is a post-doctoral Researcher and instructor at the Helsinki University of Technology. He holds a Doctorate of Science in the area of information and communications technology.

Jürgen Neumüller is Senior Consultant and co-owner of INFRASTRUKTUR & UMWELT, Potsdam. He has a Doctorate in Civil Engineering from the Technical University of Darmstadt, with a special focus on water management and regional planning.

Piia Nikula is a Researcher at the Aleksanteri Institute, University of Helsinki. She holds her Master's degree in Political Science, International Relations, and also has a BA in French.

Christer Pursiainen is Senior Research Fellow at Nordregio, Stockholm. He is a Doctor of Political Science and Docent in International Relations at the University of Helsinki.

Johanna Roto is a Researcher at Nordregio and holds an MSc with a major in Human Geography from Helsinki University, Finland, with a minor in Planning and Community Studies from Tromsø University, Norway.

Philipp Schmidt-Thomé is a Senior Scientist at the Geological Survey of Finland. He holds a PhD in Geology related to research on natural hazards, climate change adaptation and spatial planning.

Veli-Pekka Tynkkynen is Senior Research Fellow at Nordregio, Stockholm. He holds a PhD in Planning Geography, while his core expertise is in regional development and environmental planning in Russia.

EXECUTIVE SUMMARY

Critical infrastructures are systems, which are essential for the maintenance of vital societal functions, including the supply chain, health, safety, security, economic and social well-being of people. Although such systems have naturally existed for a long time, the very concept of critical infrastructure is relatively new. Its wider use as an authorised policy concept upon which programmes, action plans, legislation and so forth are built can be traced back to the United States in the mid-1990s. The related concept of critical infrastructure protection reflects the more purposeful concern of the vulnerability of critical infrastructure. After some delay, these concepts became popularised in Europe too.

All countries have their own national traditions, institutional structures, policies and strategies, vocabulary, technical and methodological approaches and so forth as to how they protect their critical infrastructures or vital societal functions against different types of risks, threats and vulnerabilities. However, with the European Commission Green Paper, published in November 2005, and Proposal for a Directive of the Council from December 2006, a European dimension has emerged in the field of critical infrastructure protection.

This development towards a more integrated European critical infrastructure protection is a clear challenge for the national models and strategies, which differ from country to country. How would it be possible to combine the national and European levels of critical infrastructure protection into a harmonised and effective strategy?

Another challenge is the regional dimension. How, in the context of the EU-27, would it be possible to take into account the particular regional cross-border effects of critical infrastructure vulnerabilities as well as the specific features – such as particular weather conditions, technological capabilities, political and administrative systems, safety culture – of European sub-regions, with a possible presence of countries which are not members of the European Union?

This study is about critical infrastructure protection in general but has a specific Baltic Sea Region perspective. It initiates discussion about the issue of whether a regional level of critical infrastructure protection would be needed as an intermediate level between the strategies of national governments and the European Union. In addition, the study offers detailed case studies in some of the most central critical infrastructure sectors, such as electricity, information and communication technology, oil transportation and maritime safety, gas pipelines, and water.

Towards a Baltic Sea Region strategy in critical infrastructure protection

Chapter I starts this inquiry by opening some perspectives onto the particularities of the Baltic Sea Region from the point of view of critical infrastructure protection. These include specific climate conditions, long distances, in some sectors and between some countries closely integrated economies, still a variety of

economic, political and administrative systems and cultures as well as institutional solutions as to international cooperation and integration, and very fragmented and multilayered regional networks.

The introductory chapter goes on by discussing the question of ‘what are critical infrastructures’. In analytic, academic and practical literature, a wide range of definitions can be found. Moreover, the definitions vary across the countries and the exact context, though they have much in common. The concept of critical infrastructure has also had different meanings at different times.

The chapter reviews some relevant official definitions of critical infrastructure in the comparative perspectives of the United States, North Atlantic Treaty Organization, the European Union, and the Baltic Sea Region countries. This overview shows that though these definitions overlap, they are also in many ways different in their exact understandings of what are the critical sectors and also in more fundamental perspective about what to focus on in their strategies.

However, while infrastructures or critical infrastructures were perhaps earlier understood as something very tangible and concrete, either physical or information and communication technology systems, there seems to be a trend towards a broad, holistic understanding of critical infrastructure, where it is understood as networks or systems of vital functions of the society as a whole, or the infrastructures embedded in, or supporting, these functions. This trend is especially visible in the Baltic Sea Region among the Nordic countries.

Another question is that of what kinds of threats the critical infrastructure should be protected against. It seems that also the threat picture is more of a variable than fixed, shifting considerably depending on the country in question and its recent experiences. The emergence of the United States and European Union approaches on critical infrastructure protection are closely connected to the threat of terrorism. However, there seems to be a trend towards approaches based on a so-called all-hazards approach while countering threats from terrorism as a priority.

This terrorism-as-a-priority-threat approach has some support in the Baltic Sea Region when it comes to what the specifically European level of critical infrastructure protection should focus on. However, many countries in the region are fundamentally basing at least their own national strategies on all-hazards approach, which somewhat complicates the harmonization of the national and European levels of critical infrastructure protection.

There is also a debate rising about focusing more on resilience than mere protection. A resilient infrastructure is a system that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored. Very often, achieving the desired level of protection is simply not cost-effective in relation to the actual threats. As full protection can never be achieved, it has been started to ask whether the money could be better spent on making the proper preparations in order to ensure a graceful degrading of the infrastructure when disaster eventually takes place. It is concluded in the introductory chapter that this is an approach which would particularly well match the general societal security approaches in at least the Nordic countries.

Another issue discussed in the introduction is that of interdependencies. It is a common feature of critical infrastructures that they are connected to other infrastructures at several different points, forming a complex and dynamic system.

It is clear that the ability to identify and analyze interdependencies is an important part of critical infrastructure protection. It is argued in the introduction that although the interdependencies are a common feature of critical infrastructure systems and often materialize via cyber connections through information and communication technology, most of them are regionally determined, that is, they are closely related to geographic proximity and integrated regional networks. This is particularly true in the Baltic Sea Region and especially in the Nordic countries, where critical infrastructures are in many sectors part of the very same Nordic infrastructure system.

The introduction also discusses ‘the dilemma of private-public partnership’ in critical infrastructure protection. While the governments have the overall responsibility for the protection of critical infrastructures, most of these infrastructures are owned and operated by the private sector. In a globalised world, national critical infrastructures are also dependent on situation of other countries’ critical infrastructures beyond the regulative power of a nation state. The dilemma is that the private parties, while ready for cooperation, resist taking measures that go substantially beyond their business continuity requirements. In most cases, the public sector cannot take the financial responsibility to protect private critical infrastructures either, whereas increasing state regulation to force the private sector to put more resources to deal with the protection or resilience of those infrastructures they own or operate is also a difficult political issue. What remains is some kind of soft regulation, that is, public-private partnership confined to mere awareness raising, information sharing and best practice exchange. This solution seems to be the case also in the European Union and in the majority of the Baltic Sea Region countries, although there are some differences between the countries as to their readiness to implement stronger regulative efforts by the governments.

Concerning the European Union’s efforts to enhance the multilateral approaches in critical infrastructure protection, the introduction reviews the Green Paper from November 2005 and the Directive Proposal from December 2006, the latter still to be adopted. As a whole the Directive Proposal seems to have found an acceptable compromise between the needs of multilateral or even supranational cooperation and coordination and the national governments’ defensive reactions against the threats to their autonomy and sovereignty in a field that traditionally has been regarded as their sole legal responsibility. The compromise limits to the joint regulation concerning the specifically ‘European’ critical infrastructures, and leaves the national infrastructures to be protected by national strategies and solutions. More far-reaching approach would probably be not acceptable by most of the Member States in the Baltic Sea Region; bottom-up approaches are preferred, although the Member States seem to be prepared to accept some soft legislative regulation and welcome more coordination.

The question then is, from the perspective of this study, whether a regional level of governance in critical infrastructure protection is needed to intermediate between the national governments and the European levels when trying in practice to deal with the extremely complex cross-sectoral and cross-border issues with multiple actors at different levels. This question is relevant especially in a region such as the Baltic Sea Region with strong presence of non-European Union countries in the field of cross-border (and European) critical infrastructures.

In accordance with the case studies of this volume, it is proposed that the specific regional conditions should be reflected in the multilateral critical infrastructure protection strategies in order them to become effective. There is therefore a need for a regional strategy of critical infrastructure protection in the Baltic Sea Region. This regional strategy could best be coordinated – in close cooperation and consent with other regional councils and networks – by the Council of the Baltic Sea States, an intergovernmental organization including all the Baltic Sea Region countries (that is, also non-European Union countries Russia, Norway and Iceland) as well as the European Commission as full members. This regional strategy should be based on full consensus of the parties, thus leaving strongly contested issues beyond its scope. Its focus should be on regional cross-border critical infrastructures as part of the infrastructures defined by the European Union as European critical infrastructure, as well as address regionally determined vulnerabilities and interdependencies of the national critical infrastructures. This strategy should be sensitive to the national critical infrastructure protection strategies, definitions and specific features of the Baltic Sea Region countries, without complicating the European Union –wide development of common standards and strategies within the European Programme for Critical Infrastructure Protection.

Electricity

Chapter II provides a detailed case study in the field of electricity. Modern society is highly dependent on electricity, telecommunications and other services delivered through complex technical systems. A well functioning technical infrastructure is important to everyday life, economic welfare and national security. In an energy intensive society, better functioning is continuously expected from the electric grid. Due to increasing energy dependence, a major blackout in urban areas would virtually paralyse the whole society.

Natural disasters, bad weather, technical failures, human errors, terrorism and acts of war may cause disturbances in the technical infrastructures of society. A common reason for long-lasting and widespread electric power system blackouts in the Baltic Sea Region is the weather. Examples include storms, blizzards, ice storms, extreme cold weather and floods.

The specific analytical angle in this chapter is that of the infrastructure system interdependencies of the rescue services in the case of electricity blackouts. Rescue services as ‘first responders’ are responsible for detection, assessment, alerting and dispatching of specialized life support and life safety assets in society. While there is a lot of experience in carrying out risk assessment and response training exercises directed to other organizations in society, relatively little attention has been paid to the potential vulnerability of the rescue services organizations themselves. Failures in critical infrastructures would undoubtedly affect their ability to carry out their duties in a negative way.

The case study focuses on Finland, with some comparison with Sweden. Emphasis is placed on the electric power systems and on steps needed to mitigate the effects of lost critical infrastructure services on the mission capability of the rescue services. Information about how the mission capability is affected by long lasting and widespread blackouts has been collected from experiences learnt from the Janika- and Pyry-storms in Finland and the Gudrun-storm in Sweden.

Several conclusions are made on the basis of these cases. First of all, they highlight the importance of independent emergency supplies for the emergency services organisations. The rescue services themselves are becoming more and more dependent on information systems, which in turn are dependent on electricity supply. Decision support and incident follow-up systems are being developed in both Sweden and Finland. These systems should be designed in such a way, that they remain at least partly operational when the normal power and communication systems fail. The sharing of experiences and ideas across nation borders becomes an important factor

The importance of securing vulnerable institutions in society during exceptional weather circumstances became apparent during both Gudrun and Pyry/Janika storms. After only a few hours of blackout, the situation may become serious, requiring immediate action by the emergency services to save lives. The distribution of drinking water and the risk of contamination must also be taken into account during prolonged blackouts.

The cases show that there can never be too much interoperability and cooperation between the organisations involved, no matter whether they are rescue service organisations or companies from the private sector. This does not only apply to exceptional circumstances, it should be a natural part of the everyday activities.

In general, the case study shows that there is a need for better preparedness. The consequences of widespread and long-lasting electricity blackouts can be reduced by improving the electricity network structure or speeding up the maintenance. As improving the network structure is expensive, a reasonable trade-off between network investments and maintenance costs is required.

Regardless of all investments in electricity networks and their better reliability continuous electricity supply cannot be guaranteed in all cases. Therefore, a better resilience is needed. There are many elements of improving resilience like having ready-made plans of how and when personnel should be called in or put in stand-by, keeping maps up to date, following weather forecasts, making deals with third parties for providing spare parts and additional equipment, cooperation with the emergency services, and so forth. The down time can be significantly reduced by increasing preparedness.

Information and communication technology

Chapter III is a case study in the field of information and communication technology. While drawing a general picture of this field and the respective vulnerabilities, the chapter's 'sub-case study' deals with the professional mobile radio network.

The ability to access, capture, store, process and distribute electronic information rapidly is today the key to the successful operation of both public and private organizations operating in any one of a range of functional sectors. As such, these capabilities are strongly correlated to national security, the raising of the standard of living and sustenance of technology-driven knowledge-based economies.

The ever increasing dependence on information and communications technology solutions represents a crucial need, which can only be met by underlying systems that function according to expectations. A subset of these

information and communications technology systems has come to be known as critical information infrastructure. Although the definition of critical information infrastructure may differ somewhat from country to country, the common perception is of them being systems that are critical infrastructures in themselves or that are essential for the operation of critical infrastructure.

The likelihood of a protected critical infrastructure continuing to function in the presence of failures and ensuing disruptions is relatively higher than an equivalent infrastructure without protection. This basic premise is the foundation for critical information infrastructure protection. It has to be noted, though, that the designation of what is a critical information infrastructure out of the many existing information and communication technology systems is never a straightforward task. This task is further complicated by the interconnectivity between the different information and communication technology systems and their inhibited reach, enabled by the migration from isolated purpose-built systems to flexible converged systems based on the Internet's borderless malleable architecture.

The chapter starts with a discussion and definitions of the central concepts of critical information infrastructure protection, such as 'threat', 'security', 'attacks' and 'vulnerability'. It notes that it is impossible to secure fully against all attacks, because of increasingly growing complexity of information and communication technology and the related interdependencies. Therefore, each organization tries to find a compromise between the level of risk and justifiable information security investment.

Threats to a critical information infrastructure may originate from a wide range of human or non-human factors. Non-human factors are those whose resulting threats cannot be directly attributed to human actions. These include natural hazards having the potential to cause direct physical destruction to critical (information) infrastructures, leading to widespread disruptions. Non-human factors include also so-called dependency disruptions, resulting from defects or flaws in hardware, software, procedures, management functions and so forth.

Threats attributed to human factors are carried out by actors whose threat actions either have a deliberate or non-deliberate (accidental) intent. The threat actors with deliberate intent have in great part put into focus the need for critical information infrastructure protection. The threat posed by hackers and crime organizations has long been recognized within the information technology security community. Hostile governments are also recognizing the increased potential of undermining adversaries by launching attacks that disable their critical information infrastructure. The threat posed by terrorists is currently the most widely publicized issue. From the perspective of non-deliberate threat actors, insiders may become unwitting threat actors due to non-deliberate or subconscious actions, such as negligence, ignorance or even inadvertently exhausting a system's resources.

Most of the nations of the Baltic Sea Region epitomize what are known as information societies, and their achievements in this regard are routinely used as yardstick by other countries. Paradoxically, highly advanced information societies are usually left exposed to new kinds of vulnerabilities. The chapter illustrates these vulnerabilities by discussing selected examples describing some realized information security threats in the region.

Regardless of these trends, it would be an exaggeration to describe the information security situation in the Baltic Sea Region as dire. The security breaches have mostly caused inconveniences, minor displeasure, some anxiety and limited monetary losses. However, the rise in Internet crime and vandalism will probably slow down the enthusiasm to move services to the net and use them.

The selected case study focuses on professional mobile radio networks, namely so-called TETRA, and especially its application in Finland called VIRVE. These networks are not just crucial in their own right; they are also crucial in ensuring the safety and security of people and other critical infrastructure. The end users of professional mobile radio tend to be professionals who depend heavily on communication tools for their work and cannot afford that these services are unavailable, particularly in moments that demand a decisive response. This includes those working in emergency services, public safety and security agencies, local government administration, disaster relief, environmental protection, utilities, industrial operations, construction sites and the management of major public events.

The critical nature of the tasks carried out by these professional users means that they cannot rely solely on less robust public (mostly commercial) communication networks for their work. The service provided by public networks is more likely to be corrupted by security breaches or be totally unavailable during critical situations. By contrast, the professional mobile networks are specifically designed to guarantee security and high service availability at all times.

After the focused case, the case study concludes with several general notions on different levels of governance. Starting with the national level, most of the countries in the Baltic Sea Region are widely acknowledged as current models of leading information societies. Accompanying this success are the multiple challenges of critical information infrastructure to ensure delivery of key services and supplies, economic stability, and maintenance of overall national security. Governments are now addressing these challenges in various policy statements and strategic plans.

However, a majority of critical information assets in market economies are under the ownership of private sector organizations, a trend mirrored across the Baltic Sea Region. Furthermore, the interdependencies between organizations are getting increasingly complex, an attribute that renders itself to critical information infrastructure protection. This complexity highlights the fact that critical information infrastructure protection is not a problem confined to information infrastructure owners, hence accentuating the need for public-private partnership frameworks. The chapter discusses this public-private partnership, which brings together all the national communities (public and private) with a potential stake in the critical information infrastructure protection efforts of early warning, detection, response, and crisis management.

Moving to the regional level, the Baltic Sea Region, the cross-border interdependencies between organizations in the region are increasingly tight, particularly from the perspective of information infrastructure. For instance, there is a fibre-based backbone infrastructure that links research and higher education institutions across several countries in the region. Similarly, multinational firms in the information and communication technology sector now own infrastructure and/or have operations that span several Baltic Sea Region countries.

These developments accelerate the need for matching regional critical information infrastructure protection efforts that also serve to complement the respective strategies being planned or implemented at a national level. The regional critical information infrastructure protection efforts could be based on the recognition of the commonality of risks (vulnerabilities, threats and assets) and the potential escalation or cascading of regional disruptions within the Baltic Sea Region. Furthermore, regional efforts could be built on the potential of the extra value accrued by having robust regional critical information infrastructure, which translates into improved regional security, trade opportunities and other economic spill-overs.

Finally, there is an international level beyond the region as the connectivity of information infrastructure has a global reach. Therefore, the threat actors are equally global in their presence and their attacks just as effective, regardless of location. Moreover, as globalization continues to take hold, the effects of a European or even global crisis now yields an even greater influence on the policies and decision-making processes of individual Baltic Sea Region countries. These realities combine to make the challenge of critical information infrastructure protection a truly international one, requiring international initiatives and programs that complement those at the regional and national levels.

Oil transportation and maritime safety

Chapter IV takes up the questions of oil transportation and maritime safety. It focuses specifically on the risks in oil transportation in the Gulf of Finland. The Baltic Sea is one of the most important passages for trade and tourism between the Nordic and Baltic countries. It has gained in importance due to the enlargement of the European Union and to the boost to Russia's economic development. Oil transportation from Russia has increased drastically with the opening of the new Russian oil terminals.

This case study examines the situation of the increasing oil transportation in the Gulf of Finland, and the present sea transport safety solutions for the region. The Gulf of Finland has not yet been faced with a large-scale oil accident. However with the average figure of shipping accidents annually being around 140 and increasing every year, the odds are that a serious accident is bound to happen.

The case study reviews the accident statistics, as well as the threat pictures perceived by the Estonian, Finnish and Russian maritime authorities. Close-calls and accidents in maritime transport are not new phenomena in the Gulf of Finland. This is due to the challenging geographical conditions of the sea, difficult weather conditions in the winter time and increasing traffic. The traffic volume is high its central parts, in international water, where the lanes of 'the motorway of the seas' are located. The combination of growing oil tanker traffic in the Gulf of Finland and the crossing fast passenger traffic between Helsinki and Tallinn cause a very high risk.

Oil transportation has to be guaranteed all the year round and their importance is highlighted in winter, when the Gulf of Finland freezes each year. This demands a special design and construction of the vessels intended to sail in the Baltic all the year round. Tanker traffic is faced with the challenges caused by the ice thickness, as well as the pressure from the ice ridges, and especially when manoeuvring in convoys led by icebreakers.

Accidents are most often of unintentional nature and caused by human error or technical failures. The main factors leading to accidents are human factors (39%) and technical failures (20%). The number of collisions has not decreased despite the many efforts to prevent them. About 60% of these accidents involve cargo vessels, 15% tankers and 12% passenger ferries.

The central role of oil transports in the region allows the possibility of political tensions, whereas the transportation and its vital role could also be seen as targets for terrorist strikes. The risks are becoming increasingly international and complex, and include dimensions concerning strikes in the places never before imagined. Imagination is one of the core attributes that should be exercised in risk mapping and prevention.

The case study further discusses the existing operative systems to regulate the maritime transport risks in the Gulf of Finland. Naturally, there exist the national vessel traffic service systems in the territorial waters of each country, which are quite similar to the air traffic control system. However, there also exists a trilateral Gulf of Finland Mandatory Ship Reporting System in between the territorial waters, which was developed to match the safety needs associated with the rapid growth in vessel traffic. In addition, to give more and precise information about the maritime traffic in the Baltic Sea, a system called the Automatic Identification System was launched. However, the significant amount of information gathered by these systems is not available to be used in real-time by the operators.

The case study states that a central innovation in the technical and practical field would be that the vessel traffic operators would have an access to the planned route of vessels in a real time. This implies that a system resembling the national vessel traffic services should be adopted in the whole Gulf of Finland area. In addition, a strict agreement on vessel traffic control procedures should be introduced.

The system would be similar to that of air traffic control. Ships would thus have to follow certain routings, announced in advance, and the maritime traffic control operators would communicate with and monitor ships to ensure they are on their designated routes. The system would also follow the near future situations and provide warnings as well as commands to ships if they are about to run to danger. Similarly, the authorities could in advance see if the announced route is suited to the tonnage and other features of the ship.

In order to create a system of this order the decision by the International Maritime Organization would be needed to make it binding according to international maritime regulations. There are no obstacles to obtaining this, but the bottleneck at the moment is the low standard of equipment on vessels, such as a lack of e-navigation readiness. Ship owners do not see the need for this equipment, without an international obligation even if basically the question concerns relatively inexpensive investments, mainly transponders.

In addition, a system of penalties regarding ships that disregard safety and reporting rules should be agreed upon. The restrictions should be severe enough to have an economic effect on ship owners. At present there is no such system, and in order to be effective this type of regulation on pain of sanctions should be enhanced throughout the whole European Union.

However, by building safety procedures and systems like those currently existing systems discussed in the case study, it is possible to cover only part of the 'safety menu' needed for a safe Gulf of Finland. The above-mentioned systems and procedures can diminish the risks entailed by growing tanker traffic but it would not eliminate them. Risk related to human factors and in many cases to the level of professionalism of ship crews, remains at about 20 % of all risks, despite what procedural and technical measures are taken.

Another much discussed issue is the need of a driving licence 'ice passport'. Solving the problem of navigating in dangerous ice conditions needs both political and technical responses and solutions. The view of the maritime authorities is that the specific geographical context of the Gulf of Finland is not thoroughly understood by the European Union authorities, or by the International Maritime Organization. The most worrying issue is not the quality of tonnage, as it was few years ago, but the quality and numbers of personnel onboard the ships. However, having a well-qualified crew is a costly business for shipping companies who may decide to prioritize their expenses differently.

Practitioner-level functional cooperation remains important. Neither safety nor security can be achieved through a one-size fits all approach. It is worth of considering too whether it can be achieved regionally. Despite common goals, safety and especially security measures remain issues that emphasize the sovereign and national decision-making in the globalised world. The case study shows that issues of sovereignty still dominate at the higher political level, but that at the more practical, lower administrative level they do not create an obstacle to deepening cooperation.

Considering the risks present in the Gulf of Finland, high marks are due for the cooperation carried out. On such a heavily used sea with high probability of oil accident, the risks are being handled exceptionally well. However, there is a need for political decisions and commitment on the level of International Maritime Organization and European Union, to give a mandate for safety cooperation to evolve further. This mandate would enhance the adoption of existing technical solutions to battle the risks of growing vessel traffic. This is necessary because it is probable that the volume of oil transports will double by 2015. A larger volume of oil transported through the Gulf of Finland will not cause a problem in itself because the size of the ships will increase. But a traffic situation with more and bigger vessels has to be controlled in a much more profound way than is the case today.

However, the authors of the case study argue that it would be too simplistic to think that cross-border action only at the level of practitioners is enough. It is important to raise the issues to the international as well as national agendas and get binding instruments e.g. in the environmental protection issues. This should be done in the same cooperative spirit as the operational cooperation.

Russia as a central player in the Gulf of Finland and as a global great power wants all decisions to go through the International Maritime Organization, thus emphasising the United Nations system rather than the European Union-Russia system. However, in most cases when Finland and Estonia have tried to operate the system according to European Union directives, Russia has not been reluctant to cooperate. This potential barrier to cooperation has been avoided thanks to good personal contacts with the Russian authorities.

The case study concludes that all in all, the Gulf of Finland countries should promote the region as a pilot area within the European Union and worldwide in the field of cross-border risks prevention in maritime transport. This would provide the citizens of the European Union in general and particularly the people living by the Gulf of Finland comprehensive safety across their borders and enhance the mutual trust that is needed in developing the safety systems and procedures even further – eventually, towards a traffic control system with high-tech navigation surveillance qualities and traffic command powers delegated to traffic control operators.

Gas

Chapter V deals with another energy source, namely gas, and particularly the planned North European Gas Pipeline. The pipeline is to be one of the largest subsea gas pipeline projects in the world and is designed to provide European Union Member States with 55 bcm natural gas from Russia annually, which will be about 8% of the predicted total gas consumption in the European Union in 2015. The company *Nord Stream*, registered in Switzerland, has been established to implement the project, in cooperation with the Russian state-owned company Gazprom, which retains a 51% majority stake-holding in the enterprise, while German energy companies, added recently with a Dutch company, are minority shareholders.

The North European Gas Pipeline is by definition a critical infrastructure, and perhaps also a ‘European’ critical infrastructure as it affects several Member States. The effects of a disruption are local and global. Local effects are gas leakages and a possible gas explosion at sea level. The global effects are possible turbulences in the gas supply and natural gas market, which could burden consumers to a certain extent.

However, the probability of terrorist attacks or natural hazards that could damage or even disrupt the pipeline is rather low. Trawling and vessels anchoring near the pipeline strings pose more of a danger.

A special issue is the chemical and conventional munitions dumped in the Baltic Sea. Experts suggest that building and operating the pipeline will not cause major risks of releasing chemical warfare agents or explosion of conventional munitions. Nevertheless, this cannot fully be excluded, even if extensive investigations are carried out prior to the laying and operation of the pipeline.

The case study argues that a critical infrastructure protection strategy should be drafted for the pipeline, focusing on how to secure and to safeguard the pipeline mainly against technological hazards as trawling or anchoring ships and to have well coordinated and effective emergency response, including the fast detection and repair of damaged parts of the pipeline.

Therefore, the case study authors propose, agreements between the operator *Nord Stream* and the affected Baltic Sea states have to be made. Since the safeguarding work and emergency response touches on the security interests of the states involved, there seems to be a need to develop institutional solutions at political level.

Although the probability of attacks and natural disasters that could harm the North European Gas Pipeline is rather low, the effect of this could be substantial taken the importance of the pipeline and the side effects concerning dumped

munitions. Therefore, in a critical infrastructure protection strategy hazard scenarios should be described and responsibilities for prevention and mitigation of the hazards should be defined.

This strategy should address following issues: securing the pipeline against trawling and anchoring vessels; safeguarding of the most vulnerable parts of the pipelines (landfalls in Vyborg and Lubmin as well as the service platform); emergency response and repair of damage to the pipeline; avoidance of side effects of building and running the pipeline related to dumped munitions.

The case study further discusses the different dimensions connected to this North European Gas Pipeline protection strategy. The political dimension comes from the fact that even if the pipeline is seen as a private sector activity, its strategic role in gas supply for the European gas market and the fact that it runs through the exclusive economic zones of five Baltic Sea states makes it a political issue.

There are also several individual issues of political and security concerns that have arisen around the pipeline project. For instance, the plan of *Nord Stream* to erect a service platform next to the Swedish island of Gotland followed an intensive public debate in Sweden. A major concern was possible intelligence collection by Russia. *Nord Stream* has tried to build confidence especially as to the use and protection of the service platform.

Major concerns about the pipeline have been expressed also by Poland, who has stated that the project illustrates an example of corridors and deals that have been decided upon above its head. The authors of the chapter state that it is important that the concerned states would find a common ground at the political level. Even if the United Nations Convention on the Law of the Sea clearly states that the pipeline operation should not be impeded, additional efforts about the relevant security issues are needed.

The case study deals also with the institutional dimension of the issue. *Nord Stream* is responsible for operating the pipeline and principally it should have highest interest in developing and implementing a critical infrastructure protection strategy in order to avoid economic losses. To avoid these losses, it has to be assumed that *Nord Stream* will take care of detecting pipeline damage continuously and the fast repair of damaged parts of the pipeline.

More complicated is the field of safeguarding and complex reactions in emergency responses that might be necessary in rare cases. Even if the risks mentioned above are low, the safeguarding of a pipeline that crosses the Baltic Sea at a length of 1,200 km is a multinational task. There must be a sound strategy developed together with experts from the affected states that concentrates on crucial points such as landfalls or pressure stations.

But firstly, the case study notes, it has to be clarified who is responsible for safeguarding the pipeline – national coast guards, private security services, national intelligence agencies? Many mainly operational questions follow, such as by which means and what information will be gathered; how this information will be stored and analysed; will it be partly shared between involved security operators and intelligence agencies?

Secondly, it has to be clarified who is responsible for emergency responses – national coast guards, private services, *Nord Stream*? – as well as who, and in what

cases, will lead the emergency response action? Of course, reaction plans and trainings are essential.

In order to find the way forward, and keeping in mind that the critical infrastructure protection of the pipeline has a political dimension, it seems advisable that the protection strategy be developed and implemented by a broader panel comprising security experts and political decision makers.

For this purpose existing bodies, such as the Council of the Baltic Sea States – as the authors of the case study propose – should be considered to see whether they could moderate the process. It would also be possible to establish a separate intergovernmental/interadministrative working structure.

Another special issue is the dumped munitions, which extend beyond the pipeline itself. Being part of the protection strategy for the pipeline track it should be discussed comprehensively in a broader forum. It is essential that all available information concerning the investigation of dumped munitions is made available and that, based on an actual evaluation of the potential risks, the need for further action is decided at a political level.

The economic dimension is crystallized in the fact that since the most significant effect of a pipeline disruption could be turbulences in gas markets, there has to be found solutions for securing gas supply by either re-routing the supply via other pipelines or assuring enough storage volume to overcome a period lasting from several days to several weeks.

The costs for securing and repairing the North European Gas Pipeline are presumably small in comparison to the revenue loss, should the pipeline be disrupted. Therefore the protection of the pipeline should be a clear task and in the interest of *Nord Stream* and the consumers that benefit from it.

The social dimension comprises the fact that the North European Gas Pipeline protection has to be directed mainly to those groups and people that would be most directly affected by accidents along the pipeline, such as fishermen, ships' crews as well as pipeline workers. The pipeline could also support information campaigns to people living along the Baltic Sea coast about what to do in case of accidents involving dumped munitions.

Finally, there is the technological dimension of the needed protection strategy. The case study states that two aspects should be taken into account: the technological opportunities in safeguarding using new technologies (cameras, satellites, sonar) as well as the vulnerabilities of pipelines to attack, which is why the access by terrorist groups to technology have especially to be continuously monitored.

Water

The last of the case studies, Chapter VI, is about clean water, and more specifically about the risks for shallow groundwater aquifers in coastal areas of the Baltic Sea. A very detailed, empirical case study, providing original data, focuses on the effects of sea water rise on groundwater aquifers in the Hanko Area in South Finland.

Lack of water, especially from high quality groundwater would mean a crisis for all relevant users, such as residents and industrial sectors. Increasing cooperation among administration, industrial and other relevant sectors on the strategies of groundwater protection is needed and can be done by increasing

awareness of an importance to protect groundwater resources, hinder pollution and remediate possibly contaminated aquifers.

The objective of the case study is to provide an overview of the potential risks of the shallow groundwater resources and water supply from both human activity and climate change, including risk management in one coast area aquifer. The results obtained from the particular object of this case study can be applied to other similar aquifers, as it outlines possible threats that would impact shallow groundwater resources, considering the implications for the management of water resources in different sectors. The specific risks and threats to a seashore aquifer are changes in present sea water level, contamination of salt-water intrusion, and future sea level rise and change in precipitation and evaporation caused by climate change.

In the empirical part of the case study, groundwater level monitoring data in two observation wells of 30 minutes intervals and the sea level monitoring data of 60 minutes intervals were produced in the Hanko case study area. Based on this data, it was – for the first time in an empirical study in Finland – observed that the sea level changes have a direct and very fast effect on the groundwater level. The effect was worse in that part of the Hanko aquifer where the permeability of sand and gravel layers was high. According to the climate change scenarios, the significant rise of sea level in the Hanko coastal area could cause problems to the water supply managements and infrastructure planning in the Hanko and in many other coast aquifer areas.

On the basis of these notions, the case study proposes a conceptual model for protection of shallow groundwater aquifer for the Hanko and other coastal areas aquifer. In order to assess the new risks and threats, it is essential to establish a new risk management scheme. The detailed plan for groundwater protection is the most significant tool in the risk assessment and risk management. The plan should be prepared accurately and all the special factors based of the vicinity of sea should be considered.

Detailed studies of stratigraphy in aquifers and groundwater flow models, groundwater recharge and discharge, in correspondence to either the present climate situation or the different scenarios due to climate change, have to be done. Also, the detailed mapping of all risks or potential risks may be constructed. Groundwater level and groundwater quality monitoring in range of the contaminant is significant. Monitoring includes also biological and microbiological monitoring, especially during long hot dry summers. New technologies in online measurements have progressed substantially in recent years, so automatic monitoring is a good option.

Concrete short and long term strategies on potential economic and environmental effects have to be taken into account. Long term investment and management plans for the infrastructure of the water supply and management, such as use of more durable material and long life span for the water supply network, can ensure capacities for the unforeseen effects of the climate change in the near future.

On a larger scale, groundwater issue is not solely local or national in the cross-border aquifer areas, such as in eastern Finland, where the groundwater aquifer from the First Salpausselkä formation extends to Russia. In this and similar cases, cooperation on the groundwater management between countries is needed.

LIST OF ACRONYMS

AC	Arctic Council
ADM	Add Drop Multiplexer
ADSL	Asymmetric Digital Subscriber Line
AIE	Air Interface Encryption
AIS	Automatic Identification System
ALCEP	Algebraic Code Excited Linear Prediction
ANSI	American National Standardization Institute
API	Application Programming Interface
APS	Automatic Protection Switching
ASCI	Advanced Speech Call Items
ATM	Asynchronous Transfer Mode
AUC	Authentication Centre
AVL	Automatic Vehicle Location
B7	Baltic Islands Network
BA	Baltic Assembly
BASREC	Baltic Sea Region Energy Co-operation
BBC	British Broadcasting Company
BCM	Baltic Council of Ministers
BCP	Business Continuity Planning
BDF	Baltic Development Forum
BEAC	Barents Euro-Atlantic Council
BER	Bit Error Rate
BOSNet	Behörden und Organisationen mit Sicherheitsaufgaben Netzwerk
BS	Base Station
BSH	Federal Maritime and Hydrographic Agency
BSPC	Baltic Sea Parliamentary Conference
BSSSC	Baltic Sea States Subregional Co-operation
BSR	Baltic Sea Region
CAGR	Compound Annual Growth Rate
CAPC	Civil Aviation Planning Committee
CAPEX	Capital Expenditure

CBSS	Council of the Baltic Sea States
CCPC	Civil Communications Planning Committee
CCTV	Closed-Circuit Television
CPC	Civil Protection Committee
CPMR-BSC	Conference of Peripheral Maritime Regions of Europe – Baltic Sea Council
CDR	Call Detail Records
CERT	Computer Emergency Response Team
CHP	Combined Heat and Power
CI	Critical Infrastructure
CI2RCO	Critical Information Infrastructure Research Co-ordination
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIR	Critical Infrastructure Resilience
CIWIN	Critical Infrastructure Warning Information Network
COFREP	Gulf of Finland Mandatory Ship Reporting System
COST	European Cooperation in the field of Science and Technical Research
CPC	Civil Protection Committee
CSIRT	Computer Security Incident Response Team
D8PSK	Differential 8 Phase-Shift Keying
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DoS	Denial-of-Service
DQPSK	Differential Quaternary Phase-Shift Keying
DR	Disaster Recovery
E2EE	End-to-End Encryption
EAPC	Euro-Atlantic Partnership Council
EC	European Commission
EC EIA	Espoo Convention on Environmental Impact Assessment in a Transboundary Context
ECI	European Critical Infrastructures
EDGE	Enhanced Data Rates for GSM Evolution
EDTN	Estonian Public Safety Digital Mobile Trunk Radio Network

EEA	European Economic Area
EEZ	Exclusive Economic Zone
EIA	Environmental Impact Assessment
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
ENPI	European Neighbourhood Policy Instrument
EPCIP	European Programme for Critical Infrastructure Protection
ERC	Emergency Response Center
ESPON	European Spatial Observation Network
ETSI	European Telecommunications Standardization Institute
EU	European Union
FAPC	Food and Agriculture Planning Committee
FAR	Fourth Assessment Report (of the IPCC)
FICORA	Finnish Communications and Regulatory Authority
FIMR	Finnish Institute of Marine Research
GbE	Gigabit Ethernet
GDP	Gross Domestic Product
GIS	Geographic Information Systems
GMSK	Gaussian Minimum-Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GSM-R	GSM-Railway
GTK	Geological Survey of Finland
GTSI	Group TETRA Subscriber Identity
GW	Groundwater
HELCOM	Helsinki Commission – Baltic Marine Environment Protection Commission
HELCOM CHEMU	The Ad Hoc Working Group on Dumped Chemical Munition
JMC	Joint Medical Committee
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technology
ICTDI	ICT Diffusion Index

IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMO	International Maritime Organization
IP	Internet Protocol
IPC	Industrial Planning Committee
IPCC	Intergovernmental Panel on Climate Change
IPSec	IP Security
IRGC	International Risk Governance Council
ISDN	Integrated Services Digital Network
ISM	Information Security Management
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Information Society Technologies
IT	Information Technology
ITSI	Individual TETRA Subscriber Identity
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KEI	Knowledge Economy Index
KR	Key Resources
LAN	Local Area Network
LUT	Lappeenranta University of Technology
MA	Maritime Authority/Authorities
MAN	Metropolitan Area Network
MARPOL	International Convention for the Prevention of Pollution from Ships; Marine Pollution convention
MBES	Multi-Beam Echo Sounders
MERCW	Modelling Ecological Risks related to Sea-dumped Chemical Weapons
MOI	Ministry of Interior
MPLS	Multi-Protocol Label Switching
MS-SPRing	Multiplex Section Shared Protection Ring
MTI	Ministry of Trade and Industry
NATO	North Atlantic Treaty Organization
NC	Nordic Council
NCF	Nordisk CERT Forum

NCI	National Critical Infrastructure
NCM	Nordic Council of Ministers
ND	Northern Dimension
NDEP	ND Environmental Partnership
NEGP	North European Gas Pipeline
NESA	National Emergency Supply Agency
NG1	Natural Gas 1
NGN	Next Generation Network
NOC	Network Operations Centre
NRA	National Regulatory Authorities
NRI	Networked Readiness Index
OAM&P	Operations, Administration, Management and Provisioning
OECD	Organization for Economic Co-operation and Development
OPEX	Operating Expenditure
OSP	Operator Security Plans
OSS	Operations Support Systems
OTAK	Over The Air Keying
OTAR	Over The Air Re-keying
PBIST	Planning Board for Inland Surface Transport
PBOS	Planning Board for Ocean Shipping
PBX	Private Branch eXchange
PC	Personal Computer
PCA	Partnership and Cooperation Agreement
PCCIP	Presidential Commission on Critical Infrastructure Protection
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PfP	Partnership for Peace
PGP	Pretty Good Privacy
PIK	Potsdam Institute for Climate Impact Research
PKI	Public Key Infrastructure
PMR	Professional (or Private) Mobile Radio
POP	Point-of-Presence
POS	Point of Sale
POTS	Plain Old Telephone Service

PPP	Public-Private Partnership
PROFIBUS	Process Field Bus
PSO	Public Sector Organization
PSS	Public Safety and Security
PSSA	Particularly Sensitive Sea Area
PSTN	Public Switched Telephone Network
PTT	Push To Talk
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RAKEL	RAdiokommuniKation för Effektiv Ledning
RAS	Rapid Alert System
R&D	Research & Development
RFID	Radio Frequency Identification
ROI	Return of Investment
ROV	Remotely-Operated Vehicle
RPR	Resilient Packet Ring
RTU	Remote Terminal Unit
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAN	Storage Area Network
SCADA	Supervisory, Control and Data Acquisition
SCEPC	Senior Civil Emergency Planning Committee
SDH	Synchronous Digital Hierarchy
SDS	Short Data Service
SFPG	Security and Fraud Prevention Group
SIM	Subscriber Identity Module
SIR	Secured Infrastructure Router
SLA	Service Level Agreement
SLO	Security Liaison Officer
SLS	Service Level Specifications
SME	Small and Medium-size Enterprise
SMS	Short Message Service
SNCP	Subnetwork Connection Protection
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSA	Special Sea Area
SSL	Secure Socket Layer

SSS	Side-Scan Sonar
STM	Synchronous Transfer Module
STUK	Säteilyturvakeskus
SwMI	Switching and Management Infrastructure
TAA	TETRA Authentication Algorithm
TDMA	Time Division Multiple Access
TEA	TETRA Encryption Algorithm
TEDS	TETRA Enhanced Data Service
TEI	TETRA Equipment Identity
TETRA	Terrestrial Trunk Radio
TIA	Telecommunications Industry Association
TUT	Tampere University of Technology
TW	Territorial Waters
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UNCTAD	United Nations Conference on Trade and Development
UPC	Union of Baltic States
VAHTI	Steering Committee for Data Security in State Administration
VASAB	Vision and Strategies for the Baltic Sea Region 2010
VIRVE	VIRanomaisVerkko
VOC	Volatile organic compounds
VoIP	Voice over IP
VPN	Virtual Private Network
VTs	Vessel Traffic Service
WEF	World Economic Forum
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
WWF	World Wildlife Fund
Y2K	Year 2 Kilo (= 2000) = ‘The Millennium bug’

CHAPTER I: INTRODUCTION

Christer Pursiainen

Nordregio

Nordic Centre for Spatial Development

1 CRITICAL INFRASTRUCTURE PROTECTION IN THE BALTIC SEA REGION¹

1.1 THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION

The concept of critical infrastructures (CI)² is relatively new. Its wider use as an authorised policy concept upon which programmes, action plans, legislation and so forth are built can be traced back to the United States in the mid-1990s. The related concept of critical infrastructure protection (CIP) reflects the more purposeful concern of the vulnerability of CI. After some delay, these concepts became popularised in Europe too. Within the European Union (EU), CIP became a more widely discussed theme in connection with the development of the European Programme for Critical Infrastructure Protection (EPCIP).

Naturally vulnerable infrastructures have existed for a long time, and they have had a central role in the public sector, not least in the military and economic sectors. In that sense CI and CIP are not new phenomena.³ Yet, the current debate on CI has raised many of the previously underdeveloped dimensions of infrastructures for more careful scrutiny. The increasing interest in CI also reflects the changing conditions of modern or post-modern societies in terms of technological development and related threat perceptions, such as cyber terrorism. There tends to be a correlation between the developmental level of society, the number and complexity of critical infrastructures and the severity of the society's vulnerability to a loss of supply (IRGC 2005; Gheorghe et al. 2006, p. 6).

The rise of the CIP in the United States

The United States' interest in CIP is usually traced to the Oklahoma City bombing in 1995, which revealed several previously unrecognised interdependencies, as the society and economy was affected far beyond the city itself. This led to the so-called Clinton initiative (Executive Order 1996) and the establishment of the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996. Its tasks were to report to the President the scope and nature of the vulnerabilities and

¹ In writing this Introduction, the author has greatly benefited from the background papers and literature reviews provided by Riikka Ikonen and Piia Nikula in particular. Also Viktoria Barthofer, Per Francke and Timo Hellenberg have contributed with information and material gathering. The sections 1.5 and 1.6 are largely based on Jyrki Landstedt's and Petter Holmström's shorter analyses written originally for their case study presented in Chapter II of this volume, and published in its original form as a working paper Landstedt and Holmström (2007).

² The acronym CI is in this study used interchangeably to refer either to 'critical infrastructure' or 'critical infrastructures'. They are treated as synonyms but the choice of the singular or plural form depends on the syntactic context.

³ For the historical long-term origins of CI, see the de Bruijne and van Eeven (2007, p. 26), its lengthy footnote 5, with reference to a body of relevant literature.

threats to the nation's critical infrastructures; recommend a comprehensive national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues raised by proposals to increase protections; and propose statutory and regulatory changes necessary to effect recommendations. The PCCIP concluded in 1997 that advanced societies rely heavily upon critical infrastructures, which are susceptible to physical disruptions and to new virtual threats. The security, economy, way of life, and perhaps even the survival of the industrialized world are dependent on the combination of electrical energy, communications and computers. These recommendations led to "Presidential Decision Directive 63" on Critical Infrastructure Protection in 1998, which established lines of responsibility within the federal government for protecting each of the infrastructure elements and for formulating an R&D strategy for improving the surety of the infrastructure. Some other events, such as 'Y2K' added to the perceived importance to develop a national CIP strategy. (PCCIP 1997; PDD 1998; see also Abele-Wigert and Dunn 2006, pp. 26-27; Moteff 2003; Hagelstam 2005; Fritzson et al. 2007, p. 31)

Naturally, the 9/11 attacks in the United States considerably reinforced these CIP efforts. The Department of Homeland Security (DHS) was established and in 2003 President George W. Bush released the "Homeland Security Presidential Directive/HSPD-7" that established a national policy for federal departments and agencies to identify and prioritise CI and key resources (KR) and protect them from terrorist attack. The following year the White House released two presidential national strategies: the "National Strategy to Cyber Security" (NSCS 2003) and the "National Strategy for Physical Protection of Critical Infrastructure and Key Assets" (NSPPCI/KA 2003). These were follow-up documents to the "National Strategy for Homeland Security" (NSHS 2002), which was released in July 2002 as a reaction to the 9/11. In 2006 the DHS released a new "National Infrastructure Protection Plan" (NIPP 2006) to outline roles and responsibilities for specific government and local agencies, and the private sector. (Abele-Wigert and Dunn 2006, pp. 315-319)

The emergence of the EPCIP

The origins of the EPCIP are similarly clearly connected to the threat of terrorism. The wider European CIP debate started in the aftermath of 9/11, followed by much more rapid development especially after the 2004 Madrid train bombs and the London bomb attacks in 2005. True, there can be found CIP-related EU documents, legislation and pre-legislative proposals already before the issue of terrorism had become the priority, especially in the field of Information and Communication Technology (ICT).⁴

However, the Madrid train bombing led the European Council to ask the Commission to prepare an overall strategy to protect CI. The Commission consequently adopted in October 2004 a Communication "Critical Infrastructure Protection in the Fight Against Terrorism" (Commission 2004), which made

⁴ These include, inter alia, the Commission Communication "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" (Commission 2000), which reflects the growing interest in cyber security issues in particular.

suggestions for enhancing European prevention, preparedness and response to terrorist attacks involving CI. This was followed by the Council Conclusion on the “EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks” (Council 2004) adopted by the Council in December 2004, which in turn led the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and to set up the Commission of a Critical Infrastructure Warning Information Network (CIWIN). By November 2005 the Commission had prepared a “Green Paper on a European Programme for Critical Infrastructure Protection” (Commission 2005b), and by December 2006 a “Proposal for a Directive of the Council on Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection” (Commission 2006a).⁵

As the protection of the vital functions of society and its related CI has traditionally been the task of governments, this European development has raised the issue of the division of labour and responsibilities between the EU and the Member States in CIP. So a new concept European Critical Infrastructure (ECI) was invented to identify those infrastructures that are not only National Critical Infrastructure (NCI or mere CI) but European wide, thus bringing added value to CIP by defining part of the traditional NCI as ECI and making the latter an object of partial supranational regulation from the side of the EU/European Commission (EC).

Still, the question of where to draw the line, or whether it should be drawn, has not been completely solved. The issue becomes more complex because in practice it might be difficult to define CI and ECI so as to satisfy the specific needs of all 27 Member States, although they all admit that functional cooperation and strategies at European level are needed.

The specific challenge of this study is to look at CIP not *only* from the perspective of the EU or Member States, but in adding another level to the debate. What is the role of European sub-regions – such as the Baltic Sea region (BSR) – in the development of CIP in the European context? Does the EPCIP provide the necessary framework for effective cross-border and multilateral cooperation and coordination, while national governments continue to take care of their traditional duties to protect the NCI? Or do we need specific regional approaches between the European and national levels, focusing on regional needs for cross-border and multilateral CIP cooperation and coordination?

While even a brief appraisal of the situation in the BSR reveals that a regional approach is not only needed, but rather it has already been established – although in a very fragmented form in terms of harmonized policies or administrative structures – the issue becomes that of how the European, regional and national levels of CIP should be combined into an effective and coordinated system.

⁵ This proposal has yet to be adopted as a Directive. For a comprehensive list of all related EU/EC official documents preceding this Directive Proposal, see the above mentioned Commission (2005b) and (2006a) introductions.

1.2 THE HETEROGENIC BALTIC SEA REGION

This book is about CIP in general, but it has a specific BSR perspective. While there are several definitions of the region, in this study it is understood – if not otherwise indicated – as consisting of Denmark, Estonia, Finland, the northernmost *Bundesländer* of Germany, Latvia, Lithuania, Norway,⁶ Poland, Sweden, and some regions of Northwest Russia⁷. (Figure 1)⁸

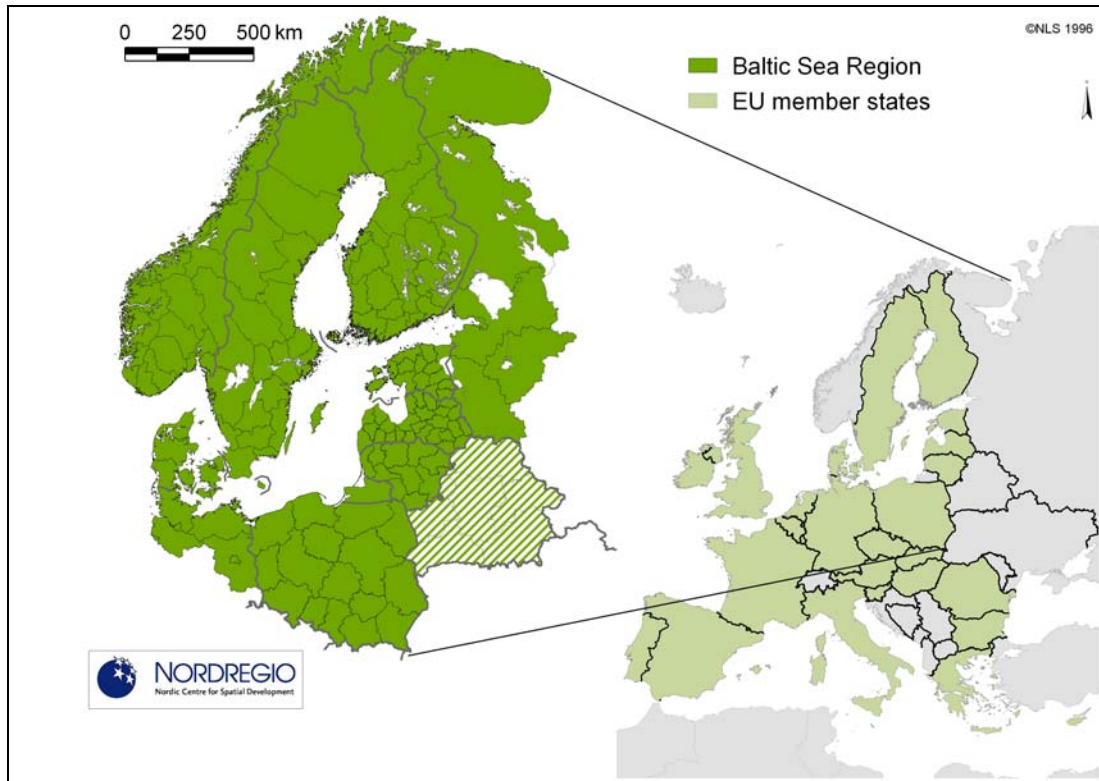


Figure I—1 The Baltic Sea Region.

⁶ Norway is almost always treated as a BSR country, even though it does not literally border the Baltic Sea. Norway is also a member of the CBSS.

⁷ The Northwest Russian regions, which are included in the BSR, also vary in different contexts; and in some EU-BSR programmes, for instance, more regions are included than in Figure 1, while sometimes the whole official administrative region of the Northwest Federal District of the Russian Federation is included. The role of Belarus is that of a kind of semi-BSR country, mainly for political reasons. While intergovernmental contacts are rather frozen and Belarus is not accepted as a member in any intergovernmental BSR institution, cooperation between regional, local or non-state actors of Belarus and other BSR countries exists; and for example the country is full eligible partner in the EU BSR Interreg IVB programme.

⁸ In some of the tables of this study Iceland is treated as one of the BSR countries. Indeed, despite the geographic distance, in Nordic connections Iceland is always treated as an equal partner, and is in many occasions, and in formal intergovernmental regional organizations, regarded as a BSR country. For instance, Iceland is a member of the CBSS.

In the European context, the BSR differs by its northern geographic location, with a relatively long winter and with strong seasonal contrasts.⁹ Cold weather has an important effect on infrastructure in the BSR. The temperature in some areas can drop to below -40°C, which can cause many problems in different infrastructure sectors. Cold weather causes the Baltic Sea to freeze for several months each year, which brings about problems for maritime transport. Heavy snow and ice is also a problem for rail, road and aviation systems, and electricity production and transmission. Higher electricity consumption during wintertime can lead to supply problems to some areas of the BSR, and even if regional cross-border markets of electricity supply work well to balance local peaks, the problems of electricity supply become obvious if large areas and several countries suffer from extreme frost simultaneously, or if there are wide network breakdowns of electricity supply due to natural, technological or man-made disasters. The failure of electricity and heating systems in cold periods would rapidly cause many economic and health problems.

In terms of land area the BSR is remarkably large compared to the rest of the EU, comprising about half of it (depending on the exact definition of the BSR). Its population is also large, numbering about 110 million people. The distribution of the population is rather heterogenic, both between and within the countries. The southern parts are densely populated whereas the peripheral northern part is more sparsely populated. (Figure 2) In general, the BSR is very much characterized by long distances between population centres, compared to the European average. Concerning population concentration, there are several big cities and growth centres in the region. (Figure 3) From this perspective, the region is characterized by the large size of St. Petersburg in particular, which is the overwhelmingly biggest city in the region.

With regard to economic development, the region is similarly heterogenic. While the Nordic countries belong to the richest of the EU-27 in terms of gross domestic product (GDP) per capita, other parts of the region do much worse by comparison. The pattern follows that of the old division between the 'West' and the 'East', as is the case in Europe in general in this respect. However, the growth rate in all BSR countries has during the past decade been higher – and in some of the eastern countries, or parts of them, much higher – than the EU average, although the total BSR GDP per capita still lags behind it. Furthermore, one can notice wide regional disparities also within those countries where economic development is otherwise beneficial. (Figure 4)

In terms of political, social and economic conditions, there are also crucial variations that reflect differences in history, culture, basic political and administrative systems (e.g. the degree of centralization vs. decentralization), economic systems (e.g. the level of market opening/liberalisation vs. state regulation), economic production structure, size, location and specific problems or challenges. Most of these issues have a direct impact on the national CIP strategies that makes a 'harmonized' approach hard to achieve.

⁹ Climate change will probably alter these basic conditions in the long run, but at the same time it brings new specifically regional climate-related problems that are important in the CIP context (HELCOM 2007). The issue of sea water rise and its effect on ground water aquifers, for instance, is discussed in detail in Chapter VI of this volume.

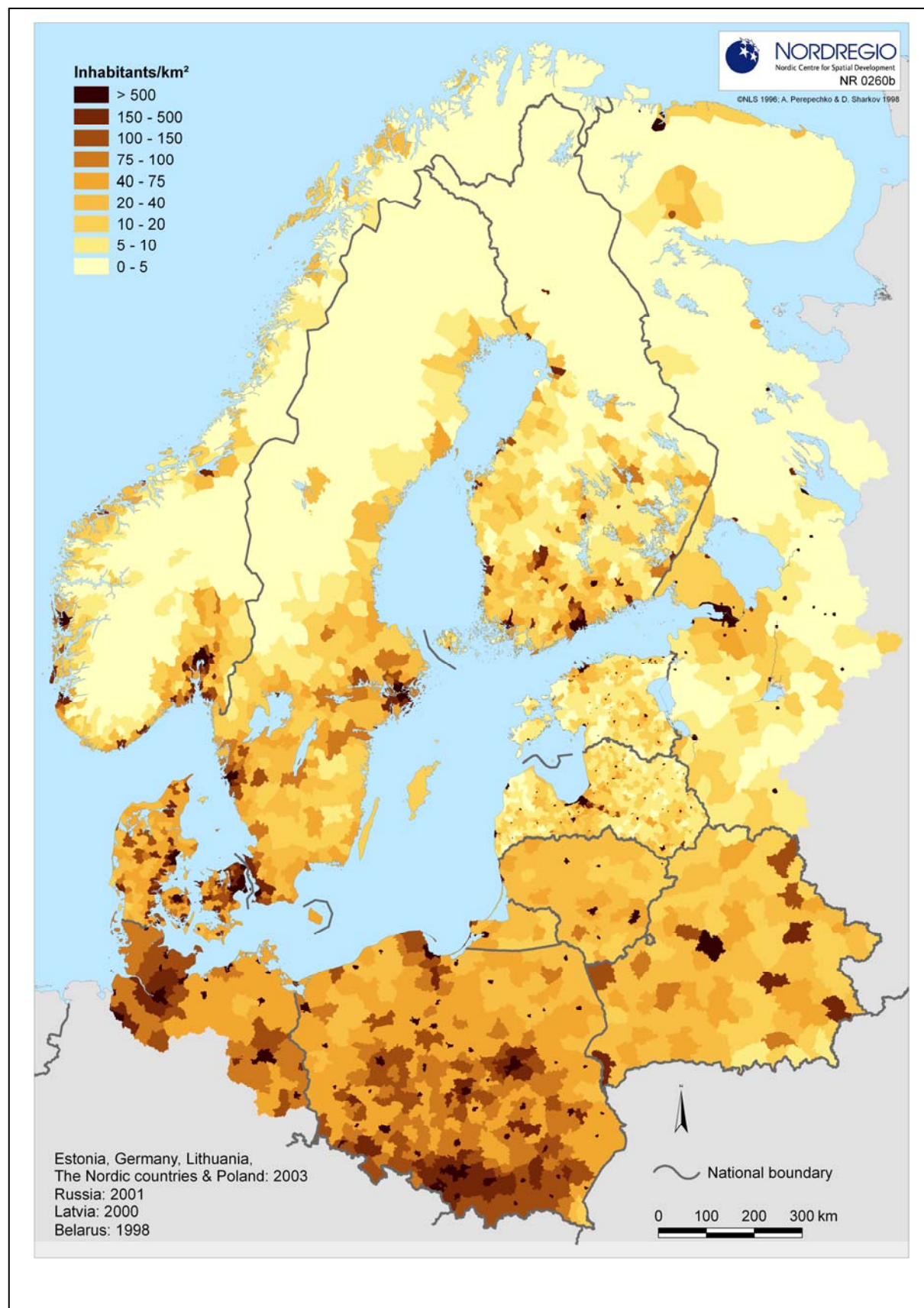


Figure I—2 Population density in the BSR.

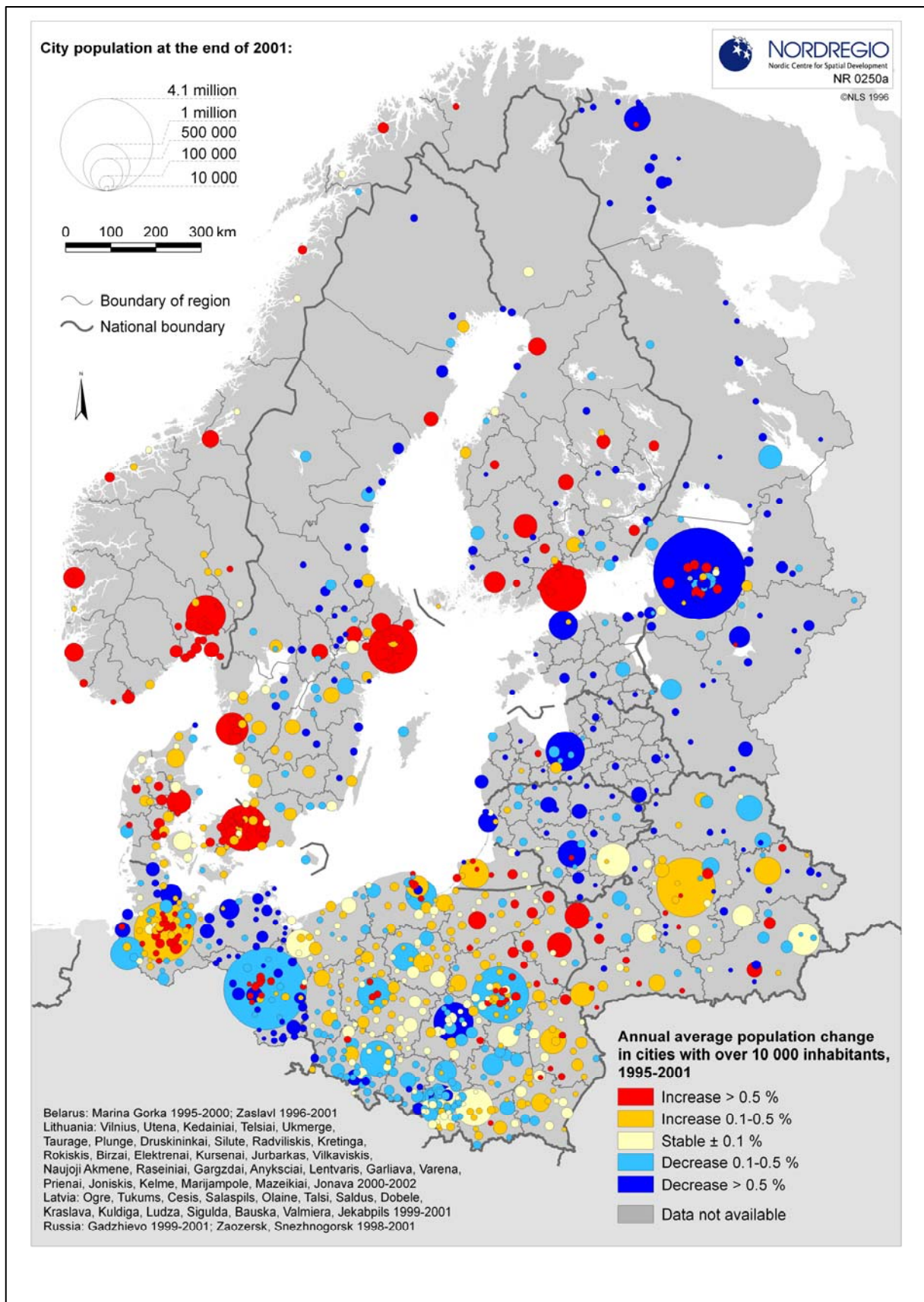


Figure I—3 City population in the BSR.

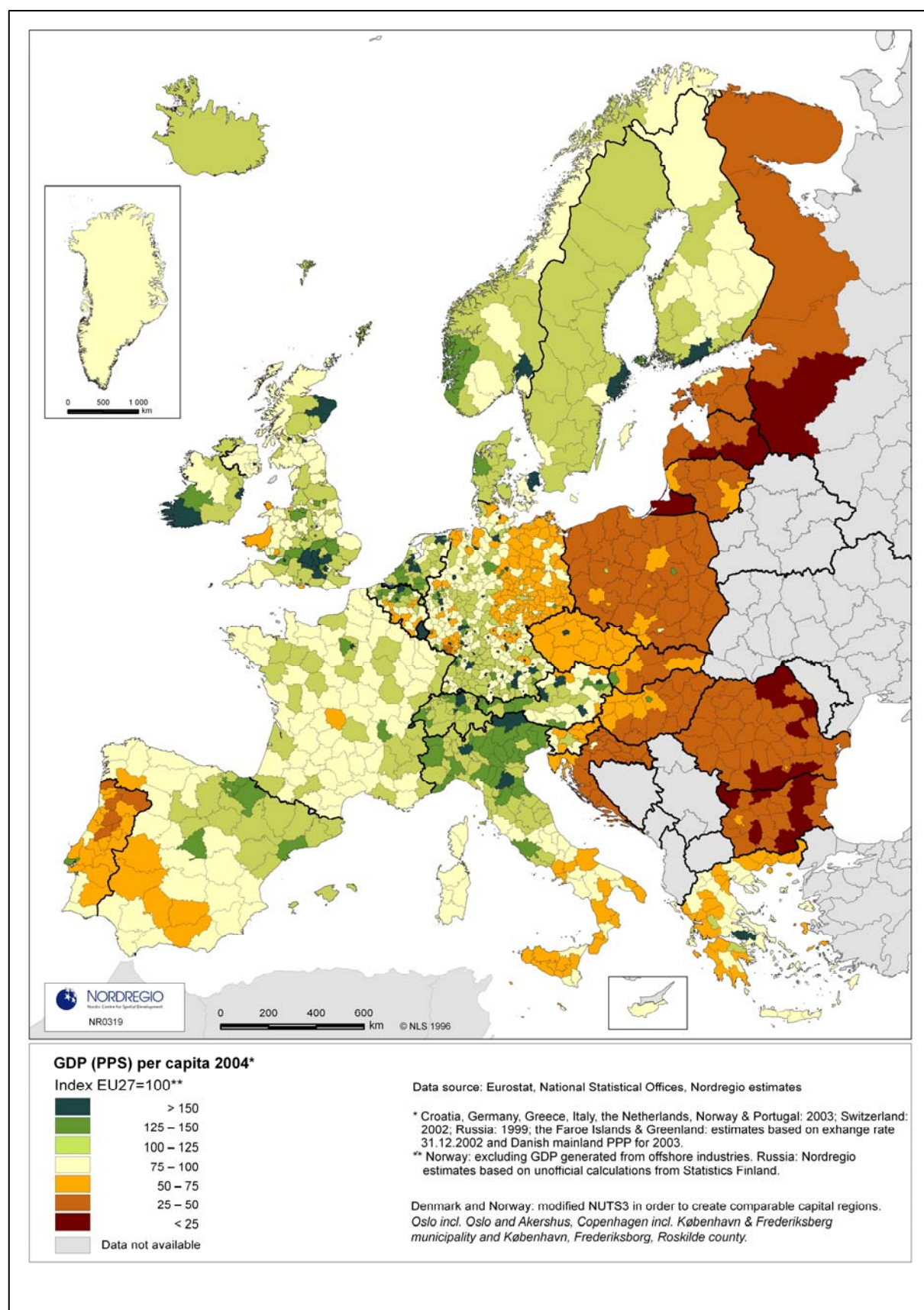


Figure I—4 GDP (PPS) per capita 2004 in Europe.

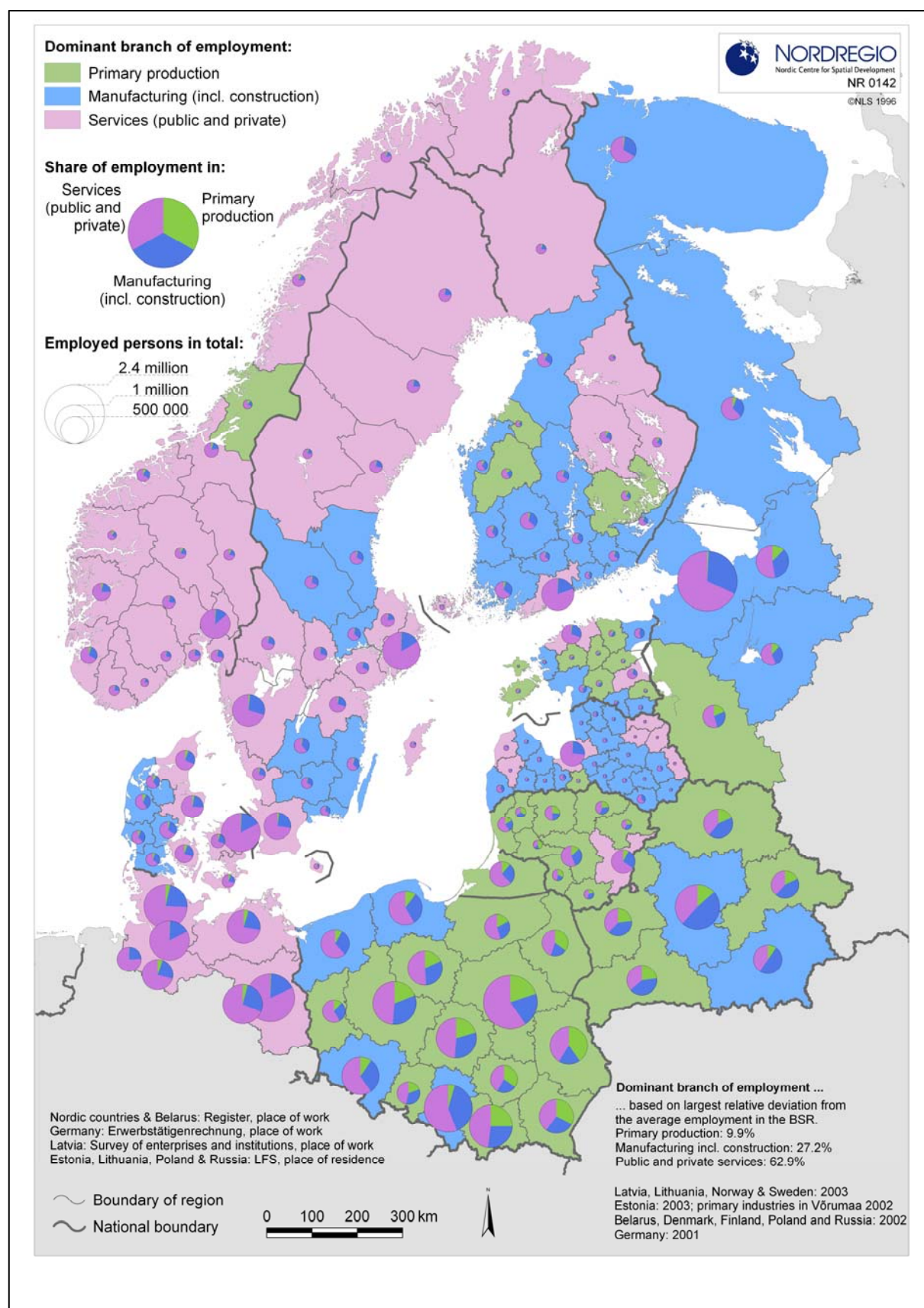


Figure I—5 Dominant branch of employment in the BSR.

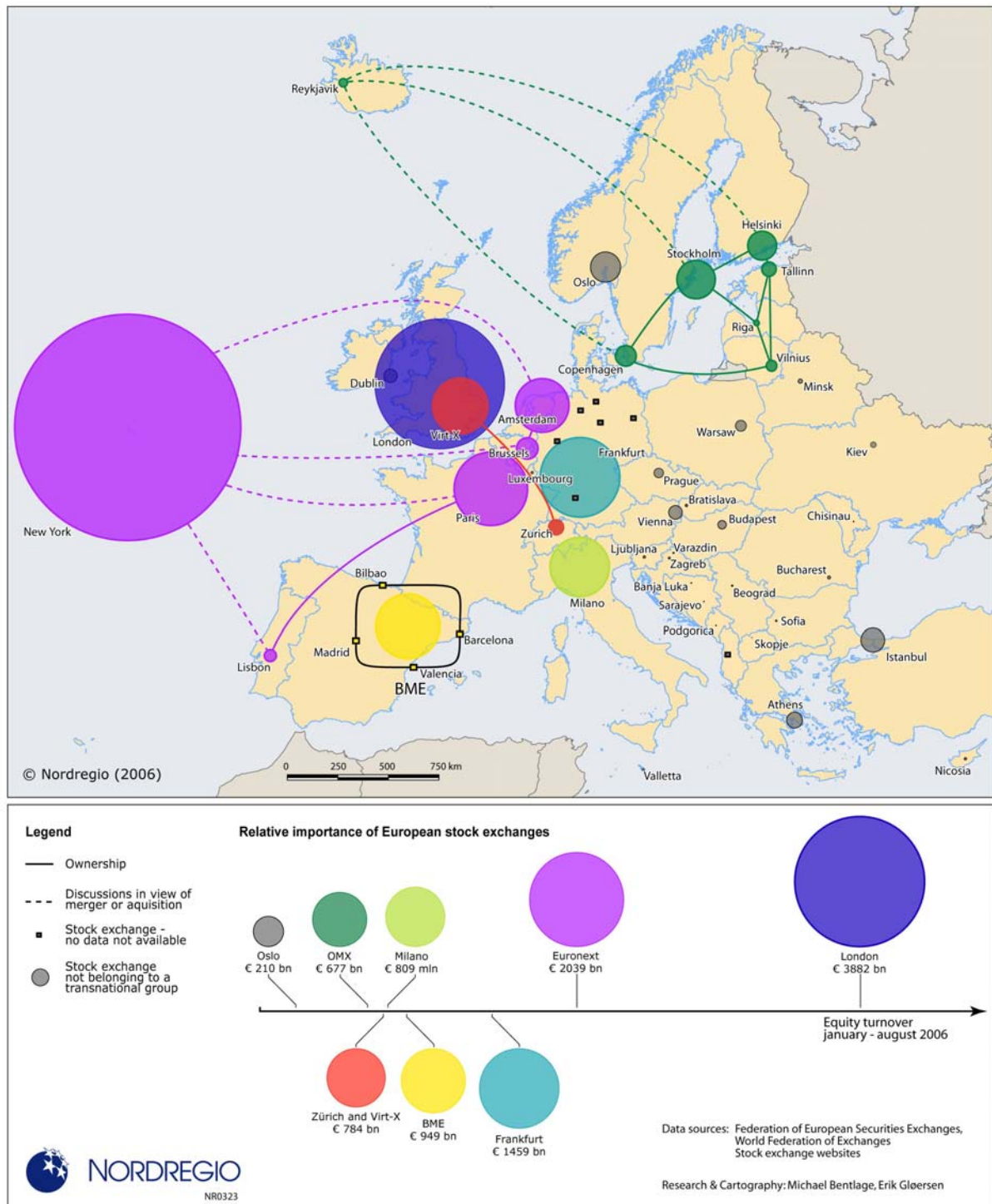


Figure I—6 Relative importance of European stock exchanges.

The region is generally regarded as one of those benefiting from globalization, although it also faces problems. All the societies in the region are characterized by a high educational level and high degree of the use of information and communication technologies (ICT). Businesses in the BSR have adapted well to the global pressures by adopting flexible strategies. Many fields of economy especially between the Nordic countries are deeply integrated, and establishing large Nordic or BSR-wide companies in such fields as ICT, flight transport or banking and financing has been a general trend already for over a decade. Yet the region looks rather heterogenic when considering its dominant branches of employment in comparative terms (Figure 5).

While being something of a success story, the BSR's relative importance in the European economy is not outstanding but remains important, the aggregated GDP being about 16 per cent of the total EU value. If measured by such criteria as stock exchange figures, it seems clear that the region is somewhat marginalized in the European economy (Figure 6). In terms of the international division of labour, the region is characterized by an image of high-tech innovation-based industries – with major ICT companies such as *Ericsson* and *Nokia* having their headquarters in the region. However, the other side of the coin from the whole BSR perspective is Russia, whose economy and especially exports is characterized by the overwhelming size of energy and other low-value-added raw materials; but in terms of CIP, this is noteworthy as Russia is a major oil and gas exporter to the European Union.

From the perspective of EU integration, this is a region with a mixture of new, old and older EU countries, plus some non-EU countries. Germany is one of the founding members of the current EU, Denmark became EU member in 1973, Finland and Sweden in 1995, and Estonia, Latvia, Lithuania and Poland in 2004. Norway has participated in the Single Market through the European Economic Area (EEA) since 1994, and in practice closely follows EU policies in many other fields, being also a non-EU member participant of the Schengen agreement. The relations between Russia and the EU are regulated by the Partnership and Cooperation Agreement (PCA) and the further development of these relations is currently supposed to take place by creating the so-called Four Common Spaces of economy, internal security, external security, and culture, science and education.¹⁰

All the BSR countries are members in the United Nations (UN) and many specialised UN-related organizations that are relevant in terms of this study, such as the International Maritime Organization (IMO), International Atomic Energy Agency (IAEA), or International Civil Aviation Organization (ICAO), and thus are parties either in various multilateral policy frameworks or regulated through them by hard and soft international law. As to North Atlantic Treaty Organization (NATO), who has its own CIP strategy (see below), Denmark, Estonia, Latvia,

¹⁰ The PCA was signed in 1994, ratified in 1997, came into force in January 1998 and was supposed to be a 10-year treaty up to December 2007. As the negotiation of a new agreement had not been able to be started between the EU and Russia due to political difficulties (Polish veto), the PCA will supposedly be prolonged a year at time until a new agreement is signed. The Four Common Spaces are: Common Economic Space; Common Space of Internal Security; Common Space of External Security; Common Space of Culture, Education and Science. Joint Road Maps have been prepared and accepted by the parties in May 2005 to enhance cooperation and regulative harmonisation in these fields.

Lithuania, Norway and Poland are members. Finland and Sweden are active participants in NATO's Euro-Atlantic Partnership Council (EAPC) and Partnership of Peace (PfP) programme, and through that participate in the organization's CIP-policies; the same goes for Russia, which however prefers to work through the separate Russia-NATO Council.

These basic categories of the BSR countries' participation in the main international organizations in the region are summarised by Table 1. However, an important refinement to this situation is that there exists a great number of intergovernmental or transnational organizations, institutions, networks, and programmes at the regional level in the BSR, most of them dealing with this or that part of CIP by any definition. This issue is discussed in some detail further on in this introductory chapter.

Table I—1 BSR countries and their participation in the EU and NATO.

BSR country Organization	Denmark	Estonia	Finland	Germany	Latvia	Iceland	Lithuania	Norway	Poland	Russia	Sweden
EU	x	x	x	x	x	EEA Schengen	x	EEA Schengen	x	PCA Four Common Spaces ENPI, INTERRE G Northern Dimension	x
NATO	x	x	EAPC & PfP	x	x	x	x	x	x	NATO- Russia Council (EAPC & PfP)	EAPC & PfP

1.3 WHAT ARE CRITICAL INFRASTRUCTURES?

The literature on CI – and on the seemingly ever-growing number of closely related concepts – forms a large body of official national documents, international organizations' documents, as well as independent researchers' and institutions' handbooks and studies. Should we start to compare the national CIP and related systems (e.g. International CEP Handbook 2006; Abele-Wigert and Dunn 2006), we would soon realise that the basic approaches, and together with them the basic definitions, of the fundamental concepts vary significantly across the countries and the exact context, though they have much in common. The concept of CI has also had different meanings at different times.

In analytic and academic literature, we can find a wide range of definitions. In surveying some of these definitions, which become broader and broader, Egan (2007, p. 5) however notices that: "These definitions aside, even the broadest of CI

systems seem to be expanding.” One main reason for this, Egan argues, is that in modern societies there exists set of systems “that are not part of the CI in their current state but which may be in the years to come.”

In this section, we discuss some relevant official definitions of CI in the comparative perspectives of the United States, NATO, the EU, and the BSR countries. We may find that though these definitions and typologies overlap, they are also in many ways different in their exact understandings of what are the critical sectors and also in more fundamental perspective about what to focus on in their strategies.

However, a general trend seems to be that while infrastructures or CI were perhaps earlier understood as something very stable and concrete, either physical or information and communication technology systems, there seems to be a trend towards a broad, holistic understanding of CI, where it is understood as networks or *systems of vital functions* of the society as a whole or the infrastructures embedded in these functions.

United States’ definition of CI

The development of the definition of CI in the United States illustrates the expansion of the concept. Moteff et al. (2003) have analysed the US debate and official documents since 1980s to the current post-9/11 Homeland Security era. While they notice that before CI became a term used in security debates, public policymakers commonly used the seemingly similar term ‘infrastructure’ as an object to be protected. However, in those early debates the concern often was the issue of ‘natural’ long-term deterioration and erosion of the important infrastructures and the need for more public funding to modernise them. When the issue became more about the ‘vulnerability’ or ‘criticality’ of those infrastructures in case of security-related rather sudden events, the criteria for an infrastructure to be judged critical became that it must be vital to one or several broad national functions.

The 1997 President’s Commission defined infrastructures as mostly the privately-owned ‘basic foundations’ for society. The report stated that:

“By infrastructure we mean more than just a collection of individual companies, engaged in related activities; we mean a networks of independent, mostly privately owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services” (PCCIP 1997, p. 3).

Moteff et al. (2003) argue that the set and number of those sectors, infrastructures or functions defined as critical or vital have been variables. Indeed, the President’s Commission 1997 focused in its report on eight infrastructures “whose incapacity or destruction would have a debilitating impact on our defence and economic security”. These eight infrastructures were telecommunication, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services and emergency services. (PCCIP 1997, Appendix 1.)

A year later, the definition was broadened and infrastructure was defined as the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution

capabilities that provide a reliable flow of products and services essential to the defence and economic security of the US, the smooth functioning of governments at all levels, and society as a whole. In this definition additional infrastructures (to those eight mentioned previously) include food/agriculture, space, numerous commodities, the health care industry and the educational system. (PDD 1998).

In the current United States approach CI is slightly different, even broader and connected to another concept, namely Key Resources (KR). The CI/KR sectors are defined in Table 2 (NIPP 2006, p. 17)¹¹ as constituting sixteen sectors.

Table I—2 CI/KR sectors in the United States.

Critical Infrastructure/Key Resource sectors in the USA
Agriculture and Food
Defence Industrial Base
Energy
Public Health and Healthcare
National Monuments and Icons
Banking and Finance
Drinking Water and Water Treatment Systems
Chemical
Commercial Facilities
Dams
Emergency Services
Commercial Nuclear Reactors, Materials and Waste
Information Technology and Telecommunication
Postal and Shipping
Transportation Systems
Government Facilities

The NATO definition of CI

When the concept of CI became more popular in European debates after 9/11, many of the basic elements of the US approaches were first transferred to Europe through the North Atlantic Treaty Organization (NATO). Thus, NATO's Civil Protection Committee (CPC) proposed and Senior Civil Emergency Planning Committee (SCEPC) accepted in 2003 a working definition for NATO's CIP action, which is expressed in the NATO/Euro-Atlantic Partnership Council (EAPC) "Critical Infrastructure Protection Concept Paper" as follows:

"Critical Infrastructure is those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national

¹¹ The original source of this table includes those sectoral US federal agencies responsible for the respective sectors, showing the cross-sectoral administrative challenge of CIP in a national context.

economy, public health and safety and the effective functioning of the government.” (EAPC 2003, Annex 1, p. 2)¹²

The definition is very wide, based on consensus between members. NATO emphasizes, however, that the CI does not follow the national confines but that their disruption or destruction will most probably have cascading effects in neighbouring countries. International cooperation is therefore needed, but the responsibility and accountability is to remain with governments.

The need to increase exploratory and definitional work on the problems that may arise following the attacks on CI has been stated by the SCEPC. NATO clearly took a coordinative and advisory role in CIP issues among the EAPC nations and provides a platform for information sharing, threat and vulnerability assessments and the exchange of best practices on CIP. NATO is also involved in training and education in ensuring that countries recognize the importance of CIP. (NATO 2006; for an overview, see Abele-Wigert and Dunn 2006, p. 363ff.)

NATO has no legislative power so the only way to influence the owners and operators of the CI – mainly the private sector – is by common action plans and the coordination of national legislative bodies. NATO’s goal is to make all EAPC countries realize the importance of CIP for their own nations and international community, and emphasize that CIP is as much as its weakest link.

European Union definition of CI

However, one can argue that the EU had by 2005 taken over the initiative from NATO to develop a multilateral European approach to CIP. The EU Commission adopted a similarly broad definition in its first main policy document, “Critical Infrastructure Protection in the Fight Against Terrorism” in 2004:

“Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the member states. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. Some critical

¹² In NATO the main responsible body for the civil emergency planning is SCEPC (Senior Civil Emergency Planning Committee). All the partners of PfP (Partnership for Peace) and of EAPC (Euro-Atlantic Partnership Council) can participate in the Committee. SCEPC has eight subcommittees that are responsible for the emergency planning for different sectors of society. These committees are FAPC (Food and Agriculture Planning Committee), CAPC (Civil Aviation Planning Committee), JMC (Joint Medical Committee), PBIST (Planning Board for Inland surface Transport), PBOS (Planning Board for Ocean Shipping), IPC (Industrial Planning Committee), CCPC (Civil Communications Planning Committee), CPC (Civil Protection Committee). In September 2001 EAPC created a working group under the CPC (CPC AHG Civil Protection Committee ad hoc group) to focus on CIP. Even if CPC is in charge of the NATO CIP action, other SCEPC working groups and committees participate in it too. CIP is considered a horizontal action and the interdependencies make cooperation between the different committees necessary. E.g. FAPC, IPC, CCOC, CAOC emphasize the relevance of CIP for their work. (Abele-Wigert and Dunn 2006, p. 363ff.)

elements in these sectors are not strictly speaking ‘infrastructure’, but are in fact, networks or supply chains that support the delivery of an essential product or service.” (Commission 2004, p. 3-4)

Table I—3 Critical infrastructure sectors according to the EU.

CI Sector	CI Sub-sector
I Energy	1 Oil and gas production, refining, treatment, storage and distribution by pipelines 2 Electricity generation and transmission
II Nuclear industry	3 Production and storage/processing of nuclear substances
III Information, Communication Technologies, ICT	4 Information system and network protection 5 Instrumentation automation and control systems (SCADA etc.) 6 Internet 7 Provision of fixed telecommunications 8 Provision of mobile telecommunications 9 Radio communication and navigation 10 Satellite communication 11 Broadcasting
IV Water	12 Provision of drinking water 13 Control of water quality 14 Stemming and control of water quantity
V Food	15 Provision of food and safeguarding food safety and security
VI Health	16 Medical and hospital care 17 Medicines, serums, vaccines and pharmaceuticals 18 Bio-laboratories and bio-agents
VII Financial	19 Payment and securities clearing and settlement infrastructures and systems 20 Regulated markets
VIII Transport	21 Road transport 22 Rail transport 23 Air transport 24 Inland waterways transport 25 Ocean and short-sea shipping
IX Chemical industry	26 Production and storage/processing of chemical substances 27 Pipelines of dangerous goods (chemical substances)
X Space	28 Space
XI Research facilities	29 Research facilities

When the EU started to develop its own European Programme on CIP (EPCIP), it had to detail and specify its definition of CI. The European Commission definition offered in the 2006 Directive Proposal states that

“Critical Infrastructure means those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people” (Commission 2006a, p. 15).

This definition is added with a specification of the sectors concerned. Compared to the US approach, the EU definition seems to be even wider and more complex, as depicted in Table 3 (Commission 2006a, Annex 1, p.21). However, as most of the

CI should be taken care of and protected by the Member States, only those CI that can be clearly identified as ‘European’ should be covered by the EPCIP. There was a lively discussion about how to define the ‘Europeaness’ of a CI. How many countries should be involved? How should one define the severity of European level disturbances if these ECI collapse or come under attack? Should the infrastructure be located in the EU area or could some CI outside the Union be CI for the EU and, if so, what would it entail? In any case, the current Directive Proposal defines ECI as follows:

“‘European Critical Infrastructure’ (ECI) means critical infrastructures which disruption or destruction would significantly affect two or more Member States, or a single Member State if the critical infrastructure is located in another Member State. This includes effects resulting from cross-sector dependencies on other types of infrastructure.”
(Commission 2006a, p. 15)

CI definitions in the BSR

If we take a look at the BSR countries, we see that their CIP terminology and definitions do not usually follow the US, NATO or EU terminology precisely. Some countries follow their own longer-term traditions and solutions adapted to new circumstances. In many BST countries the contemporary CI concept is based on the traditional total defence or civil defence systems that were built up during the Cold War.¹³ In other countries, CI-related issues were simply seen as a part of the general national emergency management system and contingency plans. It has been possible to develop these systems towards crisis management systems that take into account other types of threats and emergency situations that did not figure much on the previous agenda.

The degree of sophistication of CIP strategies and their respective definitions vary in BSR countries. In general, the Nordic countries and Germany have well-developed and detailed strategies; while in some countries CIP-related issues are dealt with within more general national security concepts or strategies, or then more developed CIP strategies are currently in the process of being developed.¹⁴ In order to depict the general features – similarities, differences, trends – of the

¹³ ‘Total defence’ usually refers to the need to take all the following five defence dimensions into account: military defence, economic defence, civil defence, social defence, and psychological defence.

¹⁴ One could say that the Nordic countries and Germany have rather specific CIP strategies, whereas the Baltic States, Poland and Russia have included these issues, to various degrees and sophistication, in their national security strategies. In Poland, a “National Plan for Critical Infrastructure Protection” is soon to be published, see: Interministerial meeting concerning critical infrastructure (2007) and Meeting with critical infrastructure operators (2007). For some of the other BSR countries not discussed here, see the “National Security Concept of the Republic of Latvia” (2002); “National Security Strategy of the Republic of Lithuania” (2002/2005); for Denmark, see National Sårbarhedsrapport (2006), Et robust og sikkert samfund Regeringens politik for beredskabet i Danmark (2005), OECD (2006); Russia’s strategies are best expressed in the “Doctrine of the Information Security of the Russian Federation” (2000) and “National Security Concept of the Russian Federation” (2000), of which the first one especially can be seen as relevant as it focuses on CII. For Russia, see also Abele-Wigert and Dunn (2006).

‘state-of-the-art’ in BSR debates in this field, we should take a brief comparative look at some most developed concepts in this region.

The country that perhaps comes closest to the EU definition, and in any case does not challenge it, is Germany. While there are several strategy-level CIP papers published in Germany¹⁵, its definition of CIP might be seen as a more simple variation of the EU definition:

“Critical infrastructures are organizations and institutions that are important to public welfare; such that failure or disruption of them will result in long-lasting supply bottlenecks, significant disturbances in public security or have other dramatic consequences. The public and private sectors can function only when critical infrastructures such as those in the following areas [in Table 4] can operate without serious interferences and provide their services.”¹⁶

Table I—4 Germany’s critical infrastructure sectors.

Critical infrastructure sector	Sub-sector
Transportation and traffic	Aviation, sea traffic, train, local traffic, inland water transportation, road system, postal system
Energy	Electricity, nuclear power stations, gas, mineral oil),
Hazardous materials	Chemical and biological substances, hazardous material transportation, arms industry
Telecommunications and information technology	
Finance & insurance	Banking, insurance, financial service provider, stock-markets
Services	Emergency, health and rescue services, civil protection, food and water supply, waste management
Public administration and justice system	Including police, customs and Federal Armed Forces
Other	Media, major research establishments and outstanding or symbolic buildings, cultural assets

As we see in Table 4, Germany’s definition includes eight main sectors with a number of sub-sectors. A slightly different approach is proposed by Finland. This country has actually never abandoned the old total defence approach but instead has developed it in new conditions. Finland’s CIP approach is called “The Strategy for Securing the Functions Vital to Society” (SSFVS 2006), which already reveals a somewhat broader view compared to the above-mentioned approaches.

¹⁵ Critical Infrastructure Protection Activities in Germany (2005); Problemstudie: Risiken in Deutschland (2005b); Problemstudie: Risiken in Deutschland (2005a); Critical Infrastructure Protection in Germany (2005); Schutz Kritischer Infrastrukturen – Basisschutzkonzept (2005); Dritter Gefahrenbericht der Schutzkommission (2006).

¹⁶ The definition quoted, and the Table 4 summarised, according to: Critical Infrastructure Protection Activities in Germany (2005). For a slightly different categorisation and more detailed treatment of the basically same sectors see Problemstudie: Risiken in Deutschland (2005b, Chapter 5).

Table I—5 Finland's vital functions to society.

Main areas	Functions	Sub-functions
Management of Government affairs	Workability of core element of the ministries and key government	
	Internal and external communication	
	Information to public and media	
	Safeguard the resources and preconditions of the judiciary	
International activity	Communication to other countries and international organisations, Finish citizens in other countries	
	Safeguarding of foreign trade	
	Participation in international crisis management, give and accept international civil protection assistance	
National military defence	Support protecting society's vital functions	
	Prevent and repel military threats	
Internal security	Public order and security, protect the basic infrastructure of society	
	Emergency services, flood control and dam safety, oil and chemical spills	
	Border management and immigration	
Functioning of the economy and infrastructure	Secure money supply, financial services, payment system	
	Financial and insurance markets	
	Availability of energy secured	Comprising fuel and power supply
	Reliable and secure electronic ICT systems	
	Electrical warning system	
	Transport	Ports and harbours Transport routs Airport
	Food supply	Supply of production inputs
	Water supply	Clean drinking water Sewerage and wastewater management
	Housing	
	Education	Key education Training of professionals Research facilities
The population's income security and capability to function	Social and health services	Hospital Health care Social welfare institutions
	Staff, pharmaceuticals, vaccines, medical supplies	
	Detection, monitoring and prevention of health risks	
Psychological crisis tolerance	Basic educational structures	
	National cultural heritage	
	State churches and other religion denominations	Diaconal work Funeral services

One could claim that the Finnish approach or definition of ‘vital functions’ (Table 5) is more comprehensive than the EU’s CIP definition. The SSFVS states that “the aim of securing the vital functions of society is to safeguard the country’s independence, preserve security in society and maintain the livelihood of the population.” As we have seen, the EU strategy focused on “those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments”. The Finnish approach focuses on the functions themselves rather than infrastructures that support them. Thus, the Finnish vital sectors are more or less the same as the EU’s – especially in the areas dealing with the ‘functioning of the economy and infrastructure’ and ‘the population’s income security and capability to function’ – but the main emphasis is on the functioning of society and government in all circumstances, not only in the protection of its critical infrastructures against extreme events. Hence one could say that Finland’s approach is much more based on ‘resilience’ – a concept discussed in more detail below – than protection.

The Estonian concept of ‘sectors of vital importance’ (Table 6) resembles the Finnish model, though it is simpler, and is so far expressed only as a part of the country’s National Security Concept.¹⁷ Moreover, in a more recent government document on the “Fundamentals of Counter-terrorism in Estonia” (2007, Art. 3.6), which includes a sub-section “Protection of Objects under High Risk of Attack and Critical Infrastructure”, the definition of CIP seems to be much more restricted and more in line with the EU approach.

Table 1—6 Estonia’s sectors of vital importance.

Sectors of vital importance	Sub-sectors
Consolidating the rule of law	
Enhancing internal security	The activities of security agencies
	Maintaining law and order
	Ensuring border security and migration control
	Crisis management and emergency services
Strengthening economic, social, and environmental security	Strengthening economic security
	Enhancing social safety
	Enhancing environmental safety

¹⁷ “National Security Concept of the Republic of Estonia” (2004, Ch. 4) includes a chapter “Protecting constitutional order and sectors of vital importance ensuring public safety”, summarised in Table 6.

The Swedish model, which is still in process, is in a similar spirit to the Finnish one, and is called “Critical Societal Functions” (SEMA 2007)¹⁸. Thus Sweden too prefers to use the concept of critical ‘function’ instead of critical ‘infrastructure’ to emphasise the broadness of the definition. While those functions, summarised in Table 7, are again largely overlapping with the EU definition of CI, though being more comprehensive, the whole spirit of the Swedish approach is, like Finland’s, more about resilience than mere protection. However, the Swedish model differs from the Finnish one by putting much more emphasis on local than government level functions, interestingly expressed already in the implicit ‘hierarchy order’ of the critical or vital functions (cf. the role of the ‘government’ vs. ‘municipal’ in the Tables 5 and 7 respectively). Although Finland and Sweden resemble each other as to their respective political and administrative systems, this difference reflects the Sweden’s rather more decentralised governance.

An important feature in the Swedish definition is that societal functions that are critical in emergencies can vary from situation to situation. It is not possible to list all functions that are critical in every situation, which is why it is important to analyse societal functions that are critical in different situations. This approach is basically what the more analytical literature calls the “consequence-oriented definition of criticality”, whereby it is less the infrastructures themselves that are critical but more the *criticality of the consequences* of infrastructure failure (Egan 2007, p. 5).

Norway’s CIP system is in a way a combination, or perhaps even a synthesis, of many approaches. As its Nordic neighbours, also Norway chooses to speak rather about critical societal functions than mere critical infrastructures. In the Norwegian approach – called “Protection of Critical Infrastructures and Critical Societal Functions in Norway” (2006)¹⁹ – both concepts are however included as elements at different levels, critical societal functions forming a more general level being dependent on infrastructures. The method, then, to define the criticality of a particular infrastructure includes three general criteria: *Dependability*, i.e. a high degree of dependability implies criticality; *Alternatives*, i.e. few or no alternatives imply criticality; and *Tight coupling*, i.e. a high degree of tight coupling (linkage) in a network implies criticality. This method is illustrated in Figure 7. This two-layer system makes it possible to limit the number of CI considerably. The combination of the Norwegian understanding of CI and critical societal functions is illustrated in Table 8.

¹⁸ See also: Risk- och sårbarhetsanalyser (2005); Threats and Risk Report (2005). However, while Sweden has rather developed CIP strategies in different fields, in practice this does not always mean that the risks are minimized. For instance, a recent (November 2007) official study on CIIP by the Swedish Emergency Management Agency shows that Sweden would be very vulnerable to attacks on CIIP or to cyber attacks against other CI such as water and electricity supply. Sveriges beredskap mot nätangrepp (2007).

¹⁹ Når sikkerheten er viktigst (2006); and its English summary: Protection of critical infrastructures and critical societal functions in Norway (2006).

Table I—7 Critical societal functions in Sweden.

Sector	Function
Energy supply	Production and distribution of electricity
	District heating
	Fossil fuels and vehicle fuels
Information and communication	Telephone services
	Internet
	Radio and TV broadcasts
	Postal services
	Production and Distribution of Newspapers
	Radio and TV
Financial services	Money transmission
	Cash access
	Private insurance and securities trading
Social insurances	Payment of sickness and unemployment benefits and the national pension system
Public health and medical services and special social services	Emergency hospitals
	Primary care
	Psychiatry
	Pharmaceutical supplies
	Infectious disease control
	Special social services for children
	Disabled persons and elderly
Protection, security and safety	Rescue services
	Police
	Courts
	Correctional institutions and SOS Alarm
	Military
	Coast guard
	Customs
Transport	Border and immigration control
	Road
	Rail
	Sea and air transport
Municipal services	Transport infrastructure management
	Drinking water
	Sewage treatment
	Street cleaning
	Public meeting places
Food	Refuse collection and roads
	Agriculture and production
Trade and industry	Distribution and control of food
	Retail
	IT operations and service
	Construction and contract work
Public administration (governance, support functions, service sector)	Guard and security services and the manufacturing industry
	National management
	Regional management and local management
	Diplomatic and consular services
	Inspection and permit services
	Expert and analytical services
	Detection and laboratory services
	Collection and provision of population data
	Meteorological services
	Training services and burial services

Table I—8 Norway's critical infrastructures and critical societal functions.

Critical infrastructures	Critical societal functions
Electrical power	Banking and finance
Electronic communication	Food supply
Water supply and sewage	Health services, social services and social security benefit
Transport	The Police
Oil and gas	Emergency and rescue services
Satellite-based infrastructure	Crisis management
	Parliament and government
	The judiciary
	Defence
	Environmental surveillance
	Waste treatment

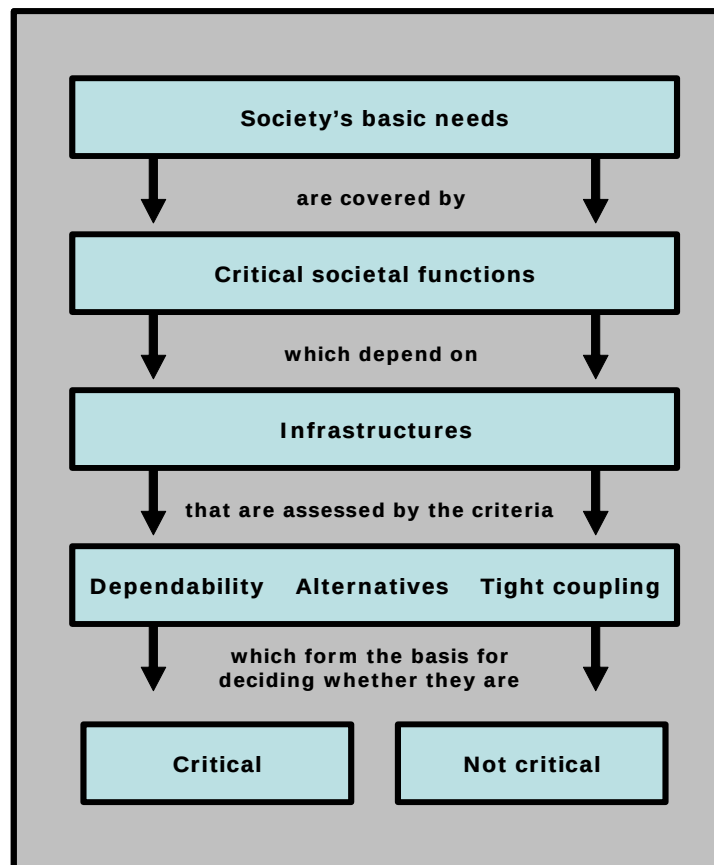


Figure I—7 The Norwegian method of defining criticality.
(Protection of critical infrastructures and critical societal functions in Norway 2006, p. 4)

This brief comparative review illustrates that the countries and organizations differ in their interpretations and definitions of what are infrastructures and how to measure their criticality. While there seem to be no antagonistic contradictions, the issue is nevertheless not only about adding this or that sector or sub-sector to the list of CI as there are more fundamental paradigmatic differences. The Nordic countries, particularly, seem to have adopted broader concepts than the EPCIP offers. This does not have to be a problem, however, if there is a way to combine these different approaches without limiting the broadness of the national concepts and widening the EPCIP concept. The Norwegian model (Figure 7) may offer a hint of how these broader functionality-based approaches could coexist smoothly, with the more limited CI approach basically matching the EU's CI definition.

1.4 PROTECTION – AGAINST WHAT?

If the above-mentioned assets, infrastructures, sectors or functions should be particularly protected, then the next question is: against what? It seems that the threat picture is more of a variable than fixed, shifting considerably depending on the country in question and its recent experiences.

Cyber threats or physical threats?

While the answer to the subtitle's question seems obvious – *Both!* – in practice finding the right balance is sometimes hard because the issue is largely affected by historical events. Each new catastrophe creates a learning process that is reflected in the CIP debates and strategies. Thus Moteff (2003) and Moteff et al. (2003) have argued that before 9/11 CIP in the United States mainly focused on cyber security. According to Moteff (2003), it was the 9/11 attacks and subsequent anthrax attacks that demonstrated the need to re-examine physical protection of CI. Indeed, while this description is open to interpretation,²⁰ if one takes a look at the key policy documents on CIP before 9/11, namely the 1997 report of the “President's Commission on Critical Infrastructure Protection” (PCCIP 1997) and the 1988 “Presidential Decision Directive” on CIP (PDD 1998), this argument can with some qualification be defended. In analyses of the implementation of the PDD implementation on the eve of 9/11 the focus was still clearly on cyber threats²¹.

Though both the above mentioned official documents carry the notion of physical threats, the spirit of them is that one should prepare in addition or perhaps in particular for previously neglected cyber threats, because of the growing technological, computerized *interdependencies* between the different functions and infrastructures. Thus, the PCCIP puts it as follows:

²⁰ This argument might be somewhat too strong, if take into consideration that e.g. Hagelstam (2005), Fritzson et al. (2007) and most others, who have traced the roots of the CIP in the United States argue (somewhat in contradiction to Moteff's claim) that the US CIP development was a direct consequence of the Oklahoma 1995 bombing.

²¹ See e.g. Moteff (2001) as an example of this kind of analysis.

“Physical means to exploit physical vulnerabilities probably remain the most worrisome threat to our infrastructures *today*. But almost every group we met voiced concerns about the new cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyber threats *before* they materialize and produce major system damage.” (PCCIP 1997, p. 5)

Consequently, the PCCIP states that it “looked at both physical and cyber threats; however, we concentrated on the fundamentally new security challenges presented by networked information systems.” (PCCIP 1997, p. 30)

This is essentially a question of whether we should speak about CIP or Critical Information Infrastructure Protection (CIIP), or what the similarities and differences of these concepts are and how are they related. Indeed, CIP and CIIP are often used inconsistently. Dunn (2006, p. 28) defines CIP as a larger concept, and the majority of methods and models are designed and used for it. Critical Information Infrastructure (CII) is then often treated as a special part of overall CI. Dunn argues further that the concepts should not be discussed as completely separate entities.

“While CIP comprises all critical sectors of a nation’s infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on the critical information infrastructure. The lesson from this seems to be that an exclusive focus on cyber-threats that ignores important traditional physical threats is just as dangerous as the neglect of the virtual aspect of the problem.” (Dunn 2006, p. 29)

Dunn and Mauer (2006) continue this line of argument by stating that CII underpins many elements of the CI, as many information and communication technologies (ICT) have become all-embracing, connecting other infrastructure systems and making them *interrelated* and *interdependent*. CII has become more important in particular due to its growing role in the economic sector, its interlinking position between various infrastructure sectors, and its essential role for the functioning of other infrastructures.

CIIP is naturally a central element of any country’s and organization’s CIP strategy (cf. Tables 2 - 8). In the EPCIP and related EU documents the cross-sectoral importance of CIIP is emphasised and the issue is seen in some respect from two perspectives. On the one hand, ICT or a large part of it is an essential CI itself due to its impact on economies and societies. On the other hand, the ICT infrastructures offer new opportunities for criminal conduct that crosses many sectors and borders and causes extensive financial damage. (Commission 2000) Consequently the EU definition of CII is:

“ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc)” (Commission 2005b).

The CIIP is defined as:

“The programmes and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of

failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.” (Commission 2005b)

While ICT/CII can be vulnerable in a multitude of ways, as will be discussed in detail in Chapter III, in most connections when CII is discussed, it is connected to cyber attacks (see Wilson 2006), supposing that there are assailants attacking from a distance through virtual channels. The object of these cyber attacks is not necessarily CII but any CI. In several EU documents dealing with terrorism this perspective is raised. The issue becomes that of the consequences of this type of attack in terms of severity, such as loss of life. One Commission document states that the consequence of an attack on the industrial control systems of critical infrastructures could vary widely:

“It is commonly assumed that a successful cyber attack would cause few, if any, casualties, but might result in loss of vital infrastructure service. For example, a successful cyber-attack on the public telephone switching might deprive customers of telephone service while technicians reset and repair the switching network. An attack on a chemical or liquid natural gas facility’s control systems might lead to more widespread loss of lives as well as significant physical damage.”(Commission 2004, p.3)

Terrorism or all-hazards approach?

The United States, NATO and EU approaches on CIP are clearly dominated by and closely connected to the threat of terrorism. In the CIP debates in the United States, the view that “We face a determined, intelligent enemy who seeks to cause us maximum harm” and therefore one should focus on worst-case analysis (Brown et al. 2006, p. 16), is clearly hegemonic. But, by way of refinement, it is useful to emphasise the different phases in the development of the CIP concept from this perspective.

If one looks at the developments of the CIP in the United States, the emphasis early on was on deliberate threats (PCCIP 1996; cf. Abele-Wigert and Dunn 2006, pp. 26-27). It is true that the so-called all-hazards approach was accepted in United States’ emergency management planning as a ‘second priority’ (Guide for All-Hazards Emergency Operations Planning 1996) and the PCCIP in a way accepts the relevance of this approach by stating that “Each of the infrastructures is vulnerable in varying degrees to natural disasters, component failures, human negligence, and willful human misconduct” (PCCIP 1997, p. 27). However, the report states that “While poor design, accidents and natural disasters may threaten our infrastructures, we focused primarily on hostile attempts to damage, misuse, or otherwise subvert them.” (PCCIP 1997, p. 31)

Naturally, after 9/11 the emphasis on deliberate attacks was hugely reinforced. The event gave reason to develop the “National Strategy for Homeland Security” (NSHS 2002), which defined three main strategic goals: to prevent terrorist attacks within the United States, reduce America’s vulnerability to

terrorism, and to minimize the damage and recover from attacks that may occur. Moreover, the main vulnerabilities and threats were now defined as chemical, biological, radiological, and nuclear weapons – i.e. physical rather than cyber attacks. This approach was later developed into the “National Strategy for the Physical Protection of Critical Infrastructures and Key Assets” (NSPPCI/KA 2003)²². But cyber threats were not forgotten either, as the “National Strategy to Secure Cyberspace” (NSSC 2003) was developed simultaneously.

These strategies were clearly dominated by a threat picture connected to terrorism. The partial come-back of the all-hazards approach in the United States CIP strategy (or CI/KY protection) came only after Hurricane Katrina in 2005 shifted the focus somewhat away from the one-sided emphasis on terrorism. In fact, after this disaster it became popular to make all-hazards comparative vulnerability analyses of threats against CI, which clearly showed that large-scale natural catastrophes, especially hurricanes, take place relatively often in the United States causing a lot of more losses than terrorism (cf. Parfomak 2005, p. 11). Thus in the current strategy of the United States formulated in 2006 the all-hazards approach is back, although the threat of terrorism still dominates:

“In addition to addressing CI/KR protection related to terrorist threats, the NIPP [National Infrastructure Protection Plan] also describes activities relevant to CI/KR protection and preparedness in an all-hazards context” (NIPP 2006, p. 11).

The reference points are the “direct impacts, disruptions, and cascading effects of natural disasters (e.g., Hurricanes Katrina and Rita, the Northridge earthquake, etc.) and manmade incidents (e.g., the Three Mile Island Nuclear Power Plant accident or the Exxon Valdez oil spill) on the Nation’s CI/KR” (NIPP 2006, p. 11).

Also NATO’s focus in CIP is on “ways to assist nations in improving their preparedness for the protection of civilian populations from terrorist attacks against critical infrastructure” (Abele-Wigert and Dunn 2006, p. 363).

If we look at the threat pictures of the European Union, it seems clear that terrorism, especially the Madrid 2004 bomb attacks, was the catalyst for launching the EPCIP in the first place. That is why in the Commission the development and coordination of the EPCIP became located in the DG Justice, Freedom and Security, which takes care of police affairs, terrorism and the like, instead of, say, the DG Environment/Civil Protection Unit.

However, when in November 2005 the Commission published the “Green Paper on a European Programme for Critical Infrastructure Protection” to be discussed by the stakeholders in the Member States, it gave three options concerning the threats: an all-hazards approach for everything; an all-hazards approach with a terrorism priority; a terrorism hazards approach (Commission 2005b, p. 3).

If one then looks at the Commission’s “Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection” (Commission 2006a)

²² For an analytic review, cf. Moteff and Parfomak (2004).

from December 2006 (still in process when writing this), a terrorism-as-priority approach was adopted, at least in the document's introductory words:

“In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection (EPCIP) and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, manmade, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but *the threat of terrorism should be given priority*. If the level of protection measures against a particular high level threat is found to be adequate in a critical infrastructure sector, stakeholders should concentrate on other threats to which they are still vulnerable.” (Commission 2006a, p. 13)²³

However, the decision mentioned here was taken already in December 2005, that is, less than a month after the Green Paper was offered for comment, and it seems that the priorities do not necessarily reflect the viewpoints of all the stakeholders. In fact, in the proposed Directive articles terrorism is not prioritised so strongly and the concept of ‘threat’ for instance is defined as “any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof” (Commission 2006a, p. 16).

If we look this issue from the perspective of the BSR, it seems clear that while the Member States are committed to the EU's anti-terrorism policies, and some Member States more than others even to the US-declared ‘war on terror’, the above quoted Commission statement – “manmade, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority” – seems not to suit BSR conditions, whereas the Directive Proposal's above quoted approach – “any indication, circumstance, or event” – would fit much better.

Deliberate threats to CI or CII, individual non-political violent acts and sabotage, criminal behaviour and organised crime, or politically motivated riots or protests that threaten public order or law, are today much more the reality in the BSR than terrorism. In fact, so far, no one has died in a modern terrorist attack in the Baltic Sea Region, although some of the countries included have suffered from terrorism. In all probability terrorism will arrive in the region at some point – indeed, as recently as September 2007 several people were arrested in Denmark suspected of planning terrorist attacks – but its effects on individual citizens' security as well as CI will likely be minimal compared to other threats.²⁴

²³ Italics added by the author of this Introduction.

²⁴ Indeed, should we compare terrorism to other external causes of death, we see that every year, more than five million people worldwide die as a result of some kind of *injury in every-day accidents, most of which could be avoided*. This accounts for nine percent of all deaths, placing injuries in the top three causes of death. In the European region injuries cause about 800 000 deaths annually. Looking at the BSR in particular, we notice that in each country thousands of deaths are caused annually by injuries in the form of different type of accidents. Moreover, for every death due to injuries there are hundreds, if not thousands, of individuals who are either hospitalised or treated in hospital emergency rooms or other healthcare facilities due to their injury. Many of these injured people suffer long-term or permanent disabilities. In addition to all

Especially CII must be constantly protected against sabotage, criminal activities and politically motivated attacks – and without a simple virus firewall any ICT system would collapse within hours because of deliberate attacks, as is discussed in Chapter III. However, the main threats to CI in general in the BSR are non-intentional, such as technological disturbances, natural catastrophes, human failures and so forth. Chapter II shows very clearly how vulnerable the electricity grid, and through that all other vital functions of society, is in the BSR especially under extreme weather conditions. Chapter IV discusses oil transportation and maritime safety, and demonstrates how hard winter ice conditions, increasing traffic volumes, human and technological failures and other non-deliberate threats form the basis of realistic risk analysis, even if the possibility of terrorism remains a low-probability risk. Also Chapter V, dealing with the North European Gas Pipeline, identifies threats that are much more plausible than terrorism, although it cannot be completely excluded. Chapter VI on ground water availability shows that one of the main climate change related consequence, namely sea water-level rise, has a direct effect on ground water aquifers in the coastal areas of the Baltic Sea.

Hence the study's case studies support the all-hazards approach to CIP, if the CIP strategy is made on the basis of well-founded risk analysis based on facts and experiences from the BSR. This would not be the same as neglecting the threat of terrorism. Terrorism is a very peculiar kind of threat in several ways as it challenges the state and society in the same intentional spirit as does war. Its most important feature from the CIP point of view in the BSR context is that while it is a low-probability risk, it at worst can have a huge negative impact in terms of losses. The worst-case scenarios of terrorism – say a large scale nuclear, biological or chemical attack – should direct the preparation, in the same way as one has to be prepared for a low-probabilistic but potentially extremely harmful technological nuclear catastrophe. From the perspective of the vital functions to the society it is however not rational to put all the efforts to prevent low-probabilistic emergencies and hazards.

1.5 FROM PROTECTION TO RESILIENCE?²⁵

Especially the Nordic countries seem to base their approaches on securing functionality rather than on protecting individual infrastructures; the current view of CIP in the EU emphasizes the protection of infrastructures and prevention of disturbances, such as disasters, and relatively little attention is paid to recovering

this human suffering, injuries are the cause of a major loss of human resources and productivity posing a great social and economic burden on society. The treatment and rehabilitation of injured persons often accounts for a large proportion of national or local health budgets. Though the total cost of injuries for any society is difficult to calculate a number of estimation methods to this effect do however exist. Thus in Sweden, for instance, it has been calculated that the annual cost, to society, caused by injuries is about 5 Million euros per 10 000 inhabitants. (Eurobaltic Guidelines 2007)

²⁵ This section is based on Jyrki Landstedt's and Petter Holmström's somewhat shorter analysis, which originally was part of Chapter II of this volume; see Landstedt and Holmström (2007).

from disasters. Indeed, from the perspective of the most recent CIP-related debates it seems that the concept of CIP is becoming somewhat outdated; the concept of CIP should be extended to Critical Infrastructure Resilience (CIR), of which CIP is an important part.

Complete protection can never be guaranteed. As Landstedt and Holmström put it, even the strongest walls inevitably fail and when this happens, swift damage control measures, recovery and reconstitution must be taken. For example, protection and resilience could be compared to a rigid stick and a flexible one, respectively. The former is harder to bend, but under severe pressure will esnap and cannot be repaired. By contrast, the flexible stick is easy to bend, always regains its shape and is hard to break. Therefore, focusing solely on CIP alone may provide a false sense of security, which can turn out to be disastrous, as has been proven many times in history. (Landstedt and Holmström 2007)

According to the CIIP Resilience Series Monograph (George Mason University 2007), “a resilient infrastructure is a component, system or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored.” Very often, achieving the desired level of protection is simply not cost-effective in relation to the actual threats. A small amount of extra protection might introduce a large amount of additional costs (as will be discussed in the following case studies in more detail).

As full protection can never be achieved, we should ask whether the money could be better spent on making the proper preparations in order to ensure a graceful degrading of the infrastructure when disaster eventually knocks at the door. As de Bruijne and van Eeven (2007, p. 24) have noticed, a fringe benefit from a more resilience-based preparation approach is that these “measures are substantially less expensive than investments in specific infrastructure upgrades to avoid certain risk scenarios which may or may not occur.” In short, these resilience measures encompass such activities or elements as protection, prevention, training, education, research, deterrence, risk-based mitigation, response, recovery and longer-term restoration. (Landstedt and Holmström 2007) It has been proposed that what is especially important here is to create ‘societal resilience’ capacity relying on joint efforts, training, continuity planning etc. of the whole society, including communities and businesses, rather than only enhancing the authorities’ capacities or control (Boin and McConnell 2007). Schulman and Roe (2007, p. 43) have argued that the key to increased reliability in relation to resilience “lies not primarily in the design of large technical systems but rather in their management.”

Landstedt and Holmström (2007) have pointed out that a good example of resilience in practice comes from the London Underground and bus bombings in July 2005. The very next day, the trains and buses were running again and the city was open for business as usual – thanks to prior resilience plans. By contrast, hurricane Katrina in New Orleans in 2005 is an example of lack of resilience. Too much emphasis had been on terrorist attacks whereas all other threats, such as natural disaster, had been sidelined. So when the hurricane hit the preparedness was far from sufficient and the results were all the more devastating. An example that especially highlights the importance of resilience over protection alone is the fact that the telecommunications infrastructure in the affected area was not only disrupted (e.g. due to power blackouts) but was completely destroyed.

As was already discussed above, especially the Nordic countries' systems seem to be based more on resilience than on mere protection, whereas in the EU approach, for instance, in the Green Paper (Commission 2005b), as Fritzson et al. (2007, 38) note, the "concept of resilience does not feature highly."²⁶ Indeed, it is true that the concept itself is not mentioned at all either in the Green Paper or the Directive Proposal (Commission 2006a); however, the same can be said on the national strategies of the BSR, even those of the Nordic countries although their functionality-based CI strategies' spirit is based on resilience rather than protection. This shows that the 'resilience-debate' has so far remained somewhat academic and is only coming onto the more practical agenda as a concept frequently used in different seminars and conferences on CIP, perhaps to be found in the texts of the next generation of more official CIP documents. Some semi-official handbooks and action plans to this effect are already available (e.g. Regional Disaster Resilience 2006).

1.6 DEPENDENCIES AND INTERDEPENDENCIES²⁷

CII interdependencies were briefly discussed above. In general, it seems to be true that "telecommunications and electric power are the most critical processes, on which virtually all the others depend" (Lukasik et al. 2003, p.7). However, it is also a common feature of all CI is that they are connected to other infrastructures at several different points, forming a complex and dynamic system.²⁸ Thus, an impact on one infrastructure may very well affect other infrastructures variously.

In order to properly analyse the vulnerability of a CI, the concepts of dependency and interdependency need to be introduced (Landstedt and Holmström 2007). A dependency is a unidirectional relationship from one infrastructure to another. Thus, the state of one infrastructure influences or is correlated to the state of the other, but not vice versa.

An interdependency is a bidirectional relationship between two (or more) infrastructures, meaning that the state of each infrastructure influences or is correlated to the state of the other(s). Egan (2007, p. 7) describes this as follows: "When critical systems are rafted together, the critical elements of each become critical elements of all because of the possibility that failure in one part of one system will be externalized to others."

²⁶ True, also the EC agrees that protection is not a panacea, but instead of bringing on the table the issue of resilience, for instance the "Critical Infrastructure Protection in the fight against terrorism" concludes as follows: "Not all infrastructures can be protected from all threats. For example, electricity transmission networks are too large to fence or guard. By applying risk management techniques, attention can be focused on areas of greatest risk, taking into account the threat, relative criticality, the existing level of protective security and the effectiveness of available mitigation strategies for business continuity" (Commission 2004, p. 5). Thus, the focus is on prioritizing protective measures instead of increasing resilience.

²⁷ Also this section is based on Jyrki Landstedt's and Petter Holmström's somewhat shorter analysis, which originally was part of Chapter II of this volume; see Landstedt and Holmström (2007).

²⁸ Cf. Gheorghe et al. (2006), p. 23 ff. for analysis; and see Ovilius (2007b) for an interesting graphic illustration of the complexity of the interdependencies.

Although one might think that single dependencies are easy to analyse and work around, this need not be the case. Some dependencies may be very difficult to discover, as this example taken from the CIIP Resilience Series Monograph (George Mason University 2007) illustrates:

“A fire at a Sumitomo Chemical Co. factory in Japan in 1993 led to an acute worldwide shortage of computer chips for months afterwards. The factory did not make computers or computer chips, but provided some 60 percent of the world supply of high-grade epoxy resin required to bond the plastic packages that hold integrated circuits.”

When dealing with interdependencies, things become even more complicated; circular snowball-effects may rapidly make a bad situation worse. For example, the electric power system requires telecommunications in order to function properly (supervision and data acquisition as well as communication between control centres and maintenance personnel). However, the telecommunication system also requires electric power in order to operate. Consequently, if the power system fails, the communication system will eventually fail, making it extremely difficult to get the power system back on line again, which in turn makes it impossible to get the communication system back on line, and so on.

In general four classes of interdependencies between or among infrastructures are considered. Following Rinaldi et al. (2001), these are:

- *Physical Interdependency:* Two infrastructures are physically interdependent, if the state of each depends upon the material products or services of the other. For example, a rail network and a coal-fired electrical generation plant are physically interdependent, given that each supplies commodities that the other requires to function properly.
- *Cyber Interdependency:* An infrastructure is cyber interdependent if its state depends on information transmitted through the information infrastructure. Cyber dependencies include the reliance of telecommunications for supervisory control and data acquisition (SCADA) systems, and information technology for e-commerce and business systems.
- *Geographic Interdependency:* Infrastructures are geographically interdependent if a local environmental event would create changes of state in all of them. Geographic dependencies include common corridors that natural gas pipelines share with electric power lines and/or telecommunications lines.
- *Logical Interdependency:* Two infrastructures are logically interdependent if the state of each depends upon the state of the other. An example of a logical dependency is the impact that oil futures have on natural gas prices and ultimately the natural gas infrastructure via changes in infrastructure investment.

As shown by the examples, interdependencies increase the risk of failures or disruptions in the affected infrastructures. According to Rinaldi et al. (2001), there are three major classes of failures:

- *Cascading Failure:* A disruption in one infrastructure causes failure in a component of another infrastructure, causing a disruption in that one as

well. This in turn may cause a failure in a third infrastructure, and so on. Thus, the failure cascades through the infrastructures like a wave, sometimes revealing new interdependencies between seemingly independent CI. For example, a failure in the natural gas infrastructure might result in a failure of a power generation unit, causing power blackouts.

- *Escalating Failure:* A disruption in one infrastructure worsens an existing independent disruption in a second infrastructure, mainly by affecting the time of recovery or restoration. For example, a disruption in a telecommunications network may be escalated by a simultaneous disruption in a road transportation network, as repair personnel and equipment are delayed.
- *Common Cause Failure:* Two or more infrastructure networks are disrupted at the same time, of some common cause. For example, during a storm, trees may crash both phone lines and power lines, causing disruptions to telecommunications and power distribution.

It is clear, that the ability to identify and analyze interdependencies is an important part of CIP. If we look at the above typologies from the perspective of the BSR, we can notice that although these interdependencies are a common feature of CI systems and often materialize via cyber connections through ICT, most of them are regionally determined, meaning related to geographic proximity and integrated regional networks. Thus, the breakdown of an electricity network is likely to affect first and foremost the interdependent local or regional CI networks, and only after that have an effect elsewhere. This is particularly true in the BSR and especially in the Nordic countries, where CI are in many sectors often part of the very same Nordic infrastructure system.

1.7 THE DILEMMA OF PUBLIC-PRIVATE PARTNERSHIP

Governments are usually legally responsible for safeguarding the CI, although most of the CI are owned, administered and operated by the private sector. This is why public-private partnership (PPP) is considered as a major issue in safeguarding national infrastructure (e.g. Abele –Wigert 2006, pp. 57-58). While in the United States private industry traditionally owns most of what is defined as national infrastructure, its share being estimated as 85 per cent, in many European countries such infrastructures as water, energy, and railway transportation have previously often solely been taken care of by the governments. However, since 1980s there has been an ongoing process of the market liberalisation and privatisation of these infrastructures. The rapid development of the predominantly privately owned and operated ICT, and other sectors' dependence on it, has further complicated the situation. This has led to a rather ambiguous situation in terms of the real authority, as described by de Bruijne and van Eeven:

“[Government authorities] may have, formally or informally, the overall responsibility for the reliable provision of services, but they lack the authority and resources to actually fulfil that responsibility.

Central governments bodies and policy makers involved in CIP to a large extent lack the technical expertise and the means to monitor or control CI operations.” (de Bruijne and van Eeven 2007, p. 24)

Globalization, with its tendency to move private companies outside the nation state, has moreover made the situation more complex from the perspective of the government control. The fact that national CI are dependent not only on other sectors but on situation of other countries’ CI complicates the situation, because no single country is either immune to effects or able to predict outcomes if neighbours suffered from serious infrastructure disruptions (cf. Mussington 2002, p. 25, 26), and thus the issue of how to organise CIP responsibilities between public and private actors becomes even more of a challenge.

Here we face the dilemma of common good. Indeed, de Bruijne and van Eeven have noticed that while PPP may seem self-evident and is celebrated by all parties, this ‘shallow consensus’ usually is broken when it becomes clear that the governments expect the private sector to make considerable investments beyond their cost-benefit calculations. As de Bruijne and van Eeven put it:

“[G]overnment argues that measures are needed to protect the public interests, but it is the responsibility of the private infrastructure owners and operators to implement these measures. The private parties, in turn, predictably resist taking measures that go substantially beyond their business continuity requirements, arguing that these threaten the viability of their business model.” (de Bruijne and van Eeven 2007, p. 24)

They claim that this dilemma leaves the government with only two options: to provide the necessary resources itself, funded from public budget; or to increase regulation. According to de Bruijne and van Eeven, the first option is mostly impossible, mainly for financial resource reasons but also for the reasons related to the necessary separation of public funding from private rent-seeking use.

The second option, adding regulation, would force the private sector to put more resources to deal with the protection or resilience of the systems they own or operate. Egan, among others, has proposed that, because markets are at present externalizing the CI risks, state regulation should mean establishing “liability rules based on the notion that organizations should internalize the costs of the risks they produce and that by internalizing them, they will make wiser choices about the technologies they use” (Egan 2007, p. 14).

However, de Bruijne and van Eeven (2007, p. 25) claim that here we would “come full circle” (from liberalisation back to state regulation). Indeed, while there might be some willingness in Europe to increase regulation in CI, in the United States this approach is traditionally been seen as unwise, presumably based on the ideological commitment to the idea that the state’s role in business should be minor. Thus, the Presidential Decision Directive concluded in 1998 as follows, for instance:

“Since the targets of attacks on our critical infrastructures would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and private sector. To succeed, this partnership

must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.” (PDD 1998, p. 2)

Indeed, the above quotation illustrates the argument of de Bruijne and van Eeven (2007, p. 25) that when governments have the two options – that of providing the necessary CIP resources themselves, or by adding state regulation – most CIP strategies propose *neither*. Instead, national CIP strategies are usually confined to the status quo by advocating mere awareness raising, best practice exchange, and soft ‘commitment power’ efforts with regard to private actors.

In a way, the PPP in CIP is a typical dilemma in that it is worse than a mere problem, as there are no good solutions available. In these conditions, government involvement in practical CIP efforts in the private sector remains rather limited, an argument widespread in more academic debates whereas given less emphasis so in practical PPP debates. As Robinson et al. (1998) notice, the natural starting point is that private industry determines investments in protecting the infrastructure from a business perspective. However, at the same time as the vulnerabilities are increasing, it has been noticed that while market liberalisation supports policies which emphasise the importance of low prices for consumers, one ‘side effect’ has been to reduce the funds available for investment in and maintenance of key assets (IRGC 2005, p. 1-2). Indeed, security has never been a design driver for market forces in their dealing with CI (Dunn 2006, p. 29-30). However, Robinson et al. propose that the key is that in order to have a proper security strategy it is important that industry has all the information it needs to perform risk assessment. The primary focus of industry-government cooperation should therefore be to share information and techniques related to risk management assessment, the identification of weak spots, plans and technology to prevent attacks and disruptions, and plans for how to recover from them.

Hurley (2000, p. 4) argues that in this cooperation the private sector’s role would be to help government authorities in risk analysis and technical issues and so help them to arrive more quickly at practical, workable solutions to real challenges. Mussington (2002, p. 31), in turn, argues that this kind of information sharing should be non-hierarchic. Decentralised, confederated response and information sharing mechanism for enhancing information assurance seems to provide a more flexible means of meeting a fast-changing threat to infrastructure vulnerability than ‘top-down’ methods of managing information assurance. However, Robinson et al. (1998) have further pointed out that in practice there are some barriers for this information sharing from the private sector side to that of the government authorities. From the private company’s point of view, collaboration may include or require passing over classified and secret materials, proprietary and competitively sensitive information, liability concerns, fear of regulation, and legal restrictions. These issues make far-reaching PPP difficult in practice.

On the other hand, Hurley (2000, p. 4) sees a possibility here. The active participation of the private sector in development of CIP strategies would help in promoting general acceptance by the private sector of any regulatory approach that

government may find necessary to adopt. In practice, according to Hurley, this PPP in the development of CIP strategies can occur in at least the following ways: providing comments on government regulations published in proposed for; participating in the work of advisory committees to government agencies; serving on voluntary groups that research and draft publications germane to ITC issues; and participating as speakers or panellists in forums.

The EU has clearly adopted the above-mentioned compromise, thus avoiding any far-reaching regulation of the private sector and confining to expressions such as ‘fully involving’ the private sector in EPCIP. The Directive Proposal of the EU Council 2006 stresses that:

“Effective protection requires communication, coordination, and cooperation nationally and at EU level involving all relevant stakeholders. Full involvement of the private sector is important as most critical infrastructure is privately owned and operated. Each operator needs to control the management of their risks as it is normally the operator's sole decision which protection measures and business continuity plans to implement. Continuity planning should respect normal business processes and logic and where possible solutions should be based on standard commercial arrangements. Sectors possess particular experience, expertise and requirements concerning the protection of their critical infrastructure. Hence, in line with the responses to the EPCIP Green Paper the EU approach should fully involve the private sector, taking into account sector characteristics and should be built on existing sector-based protection measures.”
(Commission 2006a, p. 3)

In other contexts in the Directive Proposal, it is mentioned that the EU approach is supposed to “encourage full private sector involvement” (Commission 2006a, p.13). Thus, it seems to confirm Andersson and Malm’s (2006, p. 166-167) argument that PPP in its current form as structural cooperation between ‘equal parties’ is seen by both public and private actors as the most effective way to reach their goals. For government PPP provides means of engaging the private sector in public affairs and achieving guideline and standards without having to use strict regulatory means. For private actors PPP offers a flexible way of meeting government requirements while avoiding regulation.

However, Andersson and Malm admit that there is evidence that there are *gaps* in deregulated sectors of CI, which cannot be covered by PPP. In the case studies of this volume, this problem is constantly noticed. Thus, Chapter II of this volume dealing with electricity blackouts notes that the “private sector, which is operating in the open market under hard competition, finds it difficult to invest more in preparedness than is economically justified.” Chapter IV, in turn, discussing maritime safety argues that the bottleneck at the moment is the low standard of equipment on vessels, such as a lack of e-navigation readiness. However, ship owners do not see the need for this equipment, “without an international obligation,” even if basically the question concerns relatively inexpensive investments.

Yet the basic idea of PPP is probably well accepted in all BSR countries, though their different situations and conditions may give room for variances in the

degree of regulation. Russia, for instance, is clearly more regulative in terms of its economic sectors, and although privatisation has been allowed in most economic areas within the framework of the Russian market economy, the Russian state has to be able to retain control over the key areas. For this reason the ‘sensitive’ fields remain difficult to open up to far reaching liberalisation or foreign ownership such that the strategic level of decision-making would move beyond the reach of the Russian state. (Liuhto 2007)

Another extreme is perhaps Estonia, which is often said to have implemented its economic post-socialist reform in 1990s through ‘shock therapy’, and which was “partly accomplished through adopting legislation based on liberal or limited regulation of the economy, thus depriving the bureaucracy of opportunities to intervene or easily undermine the foundation of new companies” (Laar 2007). Indeed, in Estonia’s counter-terrorism strategy it is stated - with the hint that some new regulative or cooperative PPP efforts will be perhaps adopted – as follows: “Protection of critical infrastructures that are in the possession of legal entities under private law is not regulated by the state. It is necessary to define objects under high risk of attack and critical infrastructure at the state level and establish principles for organization of their protection.” (Fundamentals of Counter-terrorism in Estonia 2006, article 3.6)

Sweden, in turn, has been characterised by “a substantial amount of mixed ownership of [...] critical infrastructures” and consequently a “great deal of government regulation has been accepted” (Lukasik et al. 2003, 79).

These differences become important when forming CIP strategies in the region, as each country seems to need more or less tailored solutions to the exact forms of the PPP.

1.8 EU AND MEMBER STATES – FINDING THE RIGHT BALANCE

As was seen above, the national models of CIP differ from that of the EPCIP at least in definitions and typologies but perhaps even in a more fundamental sense, such as whether the focus should be on protection or reliance/functionality, for instance. Several recent analyses of EPCIP, such as Fritzson et al. (2007, p. 39), have noted that there are actually “considerable uncertainties” in key areas of policy development and institutional design of the EPCIP and it in fact “is best described as a work in progress” and it is in fact “less a ‘program’ than a plan for a program.” Fritzson et al. criticize moreover that the EPCIP “although noble in intention, lacks a broad ‘vision’ or philosophy on addressing CIP.”

While this might be too strong and unfair a statement – a lot of work and thought has indeed been put into the EPCIP – it is legitimate to raise the question of how to find the right balance between the broader national and more limited European definitions and efforts, and how to define the division of labour between different levels?

Green Paper options

The EPCIP Green Paper (Commission 2005b) was a rather open and democratic process (although a rather hasty one), as it was produced in order to encourage discussion on the issues among all interested parties and stakeholders, such as Member States, owners and operators of infrastructures, and professional associations. It also seemed, at least formally, to open most, if not all, of the issues at stake to a genuine choice between the possible policy alternatives, such as that between the terrorism-as-priority approach vs. all-hazards approach discussed above.

The Green Paper proposed that EPCIP framework could function on a voluntary or mandatory basis. However, it clearly took the party of the latter in stating that only a legal framework would ensure a consistent and homogeneous implementation of CIP measures and establish clear responsibilities between the Member States and the Commission. Therefore a voluntary approach is in a sense already precluded in the Commission Green Paper.

The main goal in EPCIP is foremost to unify the definition of CIP by creating a common list of CI sectors, harmonize the system of the CIP in each country, ensure the protection on adequate and equal levels, avoid any negative cross-border effects the disruption or destruction of infrastructure in one Member State might have, and ensure that the rules of competition are not distorted within the EU internal market. This would be realized by constant monitoring and control. In addition to already existing sector specific approaches, EPCIP would offer a horizontal dimension to complement the sector-based approach. The methods used would be exchanging best practices and compliance monitoring mechanisms as well as setting common objectives, standards, codes and methodologies.

In defining CI the Green Paper proposed methods to separate national critical infrastructures (NCI or CI) from European critical infrastructures (ECI) by determining their cross border effect. The existing bilateral CIP cooperation would be complementary to the EPCIP and the ECI could be seen as involving either two or more Member States including relevant bilateral CI, or three or more Member States excluding all bilateral CI. This definition would be done on a sector-specific basis together with the Member States taking account of any potential security gaps or interdependencies. However it is stated in the Green Paper that identifying any infrastructure as ECI would *not* require any additional protection measures but instead solely bilateral agreements *could* exclude the Community. CI originating outside EU should also be taken into consideration – although the Green Paper does not elaborate this issue – as well as the interdependencies between the ECI.

Regarding the national CI the Green Paper saw a common European framework of protection as being particularly useful, since nowadays the majority of companies operate across borders. EPCIP would not only simplify matter for companies but also avoid them from additional costs. Here the Commission proposes the following alternatives: to integrate NCI fully within EPCIP; to leave NCI outside the scope of EPCIP; or to leave it fully up to Member States to decide whether to use parts of EPCIP in relation to NCI. In addition the Green Paper suggested either to have a single overseeing body or a national point of contact dealing with the implementation of EPCIP but leaves this issue open for discussion among the stakeholders.

As for the implementation of ECI the Commission suggested Member States to take the lead on it (e.g. in formulating identification criteria, setting up the priority sectors and minimum protection measures), together with the CI owners, operators and users. In addition their role would be in notifying of the critical nature of the infrastructure to a specific CIP body, appointing a Security Liaison Officer to work in between of the relevant bodies (owner/operator and CIP body), starting up and following an operator security plan with permanent and graduated security measures and participating in planning of civil protection.

The Green Paper suggested several key principles: *subsidiarity* emphasizing the national responsibility and giving the Commission floor only in the cases with EU cross border effect *complementarity* utilizing existing structures and measures in CIP; *confidentiality* accentuating the delicate nature of information relating to national CIP; *stakeholder cooperation* giving all relevant parties role in cooperation and contribution to CIP in all levels, although leaving the leadership to Member State authorities; *proportionality* applying appropriate protection measures focusing on areas of greatest risk and taking into account the cost-benefit ratio.

The EPCIP would also need supporting measures such as the CIWIN for which the Green Paper suggested three options. It could either work as a forum focused on the exchange of CIP ideas and best practices for the CI owners and operators where the Commission would gather and disseminate the relevant information; as a rapid alert system (RAS) of the immediate threats linking the national level to EU level; or as a combination of the previous two, that is, a communication and alert system however each having its own role. CIWIN should be complementary to the existing networks and avoid overlapping as well as offer harmonized methodology for classifying the alert levels and threats that now vary widely in different Member States.²⁹

It is suggested that the overall evaluation and monitoring of the programme be done as a comprehensive process covering all stakeholders and levels of action (EU, national). The options proposed are: to establish a peer evaluation mechanism for the Member States and Commission to work together; have the Commission report yearly on the progress made; or have the evaluation and monitoring done nationally where the CIP body would monitor the EPCIP implementation.

The comments of different Member States on the Green Paper are not provided from the Commission “due to the sensitivity of the CIP issues involved (security concerns).” The information from the Commission stated that the Member States and most of the industry involved in the in the Green Paper consultation process specifically asked the Commission not to disclose the

²⁹ The EU CIWIN system would be rather similar to the United States equivalent, CWIN – Critical Infrastructure Warning Information Network that was initiated in 2005 (ODP Information Bulletin 2005) and works under the Department of Homeland Security (DHS). CWIN works as a tool allowing communication between state and local government, other federal agencies, private sector and international organizations in case of primary methods of communication being unavailable (US DHA 2006). However, it is still unclear whether this would be the purpose of European CIWIN as well, to work as a type of urgent emergency line.

responses, as they considered them sensitive and not for the general public (Ovilius 2007a).

However, some of the Member States and especially industry representatives have published their comments on their websites. These comments are mostly favourable with the general sense on the Green Paper. The EU efforts to build a common framework are supported. To illustrate the spirit of the comments, Denmark (Denmark's response 2006), for instance, summarizes the Danish sectoral associations' comments and then answers one-by-one to the Green Paper alternatives. While basically supportive to the Green Paper principles, it, for instance, notes that "There is a need to specify what 'all-hazards approach with a terrorism priority' entails, especially regarding how other disasters than terrorism can be included in EPCIP." Denmark strongly supports the 'sector-by-sector' approach suggesting that successful CIP requires "tailor-made solutions rather than general legislation." Moreover, the principle of subsidiarity means that "national critical infrastructure is outside the scope of EPCIP and should remain so."

In a "Non-Paper on the Step-By-Step Approach to the European Programme for Critical Infrastructure Protection" (2006) a group of Member States, namely Denmark, The Netherlands, Sweden, United Kingdom, and Poland, showed that they have agreed on certain principles as to the EPCIP. They "acknowledge" and "welcome" the Commission's initiative and "support" its overall goal. The paper rather aims to propose an implementing strategy to the EPCIP by suggesting a step-by-step approach consisting of two 'workstreams', that is, practical middle-term goals. As we will see below, this idea was basically adopted as the implementation strategy for the EPCIP.

Also most of the various industrial national or international sector-associations³⁰ are rather positive, though some of them raise also critical issues. Thus, the Finnish Energy Industry (Energiateollisuus 2006), presumably reflecting Finland's more reluctant approach to EPCIP more widely, did not welcome the very idea of the Green Paper, but sees that infrastructures are nationally regulated and should remain so. "It is reasonable to ask what is a EU-level critical infrastructure. Physically vital functions are the property of Member States and companies, which means that the whole protection programme should be constructed from within the Member States towards the EU [and not the other way round]." This response is also critical towards the Commission line which according to it does not enough consider geographic and regional particularities.

Some industrial sector associations, such as the European Sea Ports Organisation (ESPO 2006), prioritising to focus only on terrorism, emphasised the need for the uniform conditions and EU standards for port security, that is, identical CIP measures to avoid distorting effect on the market through different protection regimes for identical infrastructure. Also non-EU actors were addressed, such as American Chamber of Commerce to the European Union (American Chamber 2006), who instead supported the establishment of the EPCIP "all-hazards approach with a terrorism priority". While the principles presented by the Commission were acceptable and the CIP cannot be left only on voluntary measures by different industries, the chamber emphasized that protective measures

³⁰ See Energiateollisuus (2006); EICTA (2006); ESPO (2006); FECC (2006); UITP (2006); AISCAT (2006).

and costs should be proportional to the threats. Moreover, the standards developed at EU level should not result in non-tariff barriers.

Directive Proposal

The Commission in its “Directive Proposal on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection” (Commission 2006a) had understandably a rather difficult task to harmonize the contradictory expectations from the Member States and other stakeholders.

As proposed by the Green Paper, the directive proposal confirms the protection of ECI sector by sector. This way the existing sector based measures can be complemented instead of creating new standards. The Green Paper proposed voluntary measures in the CIP as one alternative but in the directive they are not considered as adequate protective measures. Only by way of legislation can the division of labour with the stakeholders, the identification and the adequate levels of protection of ECI as well as the stability of the Internal Market be guaranteed. The process of the sectoral definition of the need and methods of protection, which has been started in transport and energy issues, has remained non-transparent.³¹

The responsibility for taking the actual protective measures remains in the Member States, and especially in the sector of (private) owners and operators. Here too the approach is sectoral and complements already existing sector-based protective measures, i.e. respective directives, regulations, Council decisions and standards.

The Directive Proposal is based primarily on the principles of *subsidiarity*, *complementarity* and *proportionality* proposed in the Green Paper. The Directive Proposal is consistent with the subsidiarity principle since the necessary CIP (or ECIP) measures to be undertaken cannot be taken by any single EU member state but must be addressed at EU level. Measures must also complement existing national protective measures and cannot go beyond what is necessary.

The Directive Proposal therefore compels the Member States to do the identification of their CI and ECI, implement the basic security measures for them and participate in the basic EU level coordination mechanism. The use of a Directive (proposal) will also, as stated, take into account the different national approaches to the CIP and different legal systems. The Directive Proposal identifies so-called crosscutting and sectoral criteria in the identification of ECI, according to the severity of the disruption or complete destruction of the ECI.³²

³¹ The Commission has pointed to the transport and energy sectors as the immediate priorities for action and consequently the DG Energy and Transport has already adopted a communication on “Protecting Europe’s Critical Energy and Transport Infrastructure”. At the website of DG Energy and Transport it is said, however, that “Given the sensitivity of the contents of the document, it is not available to the public” (Commission 2007). There is, however, a power point presentation available, see Commission (2006b).

³² Basically, there are at least three concepts, namely ‘severity’, ‘criticality’ and ‘risk assessment’, which come very close to each other. The Commission uses all of them, but the Directive Proposal explicitly defines that the severity of the consequences of the disruption or destruction of a particular infrastructure should be assessed on the basis, where possible, of the following effects: 1) Public effect (number of population affected); 2) Economic effect (significance of economic

As in the Green Paper, the Directive requires the establishment of the Operator Security Plans (OSP) which aim is to identify the ECI owners' and operators' assets and establish relevant security solutions for their protection. In addition, the OSP should include a risk analysis based on major threat scenarios, vulnerability assessment based on common methodologies as well as identification, selection and prioritisation of counter-measures and procedures divided between permanent (such security measures which cannot be installed at short notice) and graduated security measures (activated based on the prevailing risk and threat level). It is up to the Security Liaison Officer (SLO), appointed by ECI owners/operators, to function as the contact point in providing all the relevant security information between the ECI and the member state authority. The CIP Contact Point instead coordinates the information between the Commission, the Member State itself and other Member States. In all information exchange and sharing confidentiality is regarded as crucial.

While it might be said that the EPCIP is a typical technocratic and bureaucratic – if not top-down – approach to face common problems, as a whole the Directive Proposal seems to have found an acceptable compromise between the needs of multilateral or even supranational cooperation and coordination and the national governments' defensive reactions against the threats to their autonomy and sovereignty in a field that traditionally has been regarded as their sole legal responsibility. True, in reality several multilateral and EU regulations and coordination issues have a long time have to been taken into account in national CIP efforts.

The Commission has prepared the implementation strategy for the Directive by proposing a EPCIP Action Plan, which would consists of three 'workstreams', much along to the lines proposed in the above-mentioned 'Non-Paper', defined as

loss and/or degradation of products or services); 3) Environmental effect; 4) Political effects; 5) Psychological effects; 6) and Public health consequences. Each Member State then identifies those infrastructures which satisfy the criteria and notifies the Commission. (Commission 2006a) The 'criticality', in turn, is a widely discussed and somewhat flexible concept, as already seen when reviewing the different definitions of CI. The International Risk Governance Council (IRGC), for instance, states that criticality of infrastructures depends on several factors as well as on perception of the individuals. Moreover, governments have different priorities and criteria for classifying infrastructures that can be different than the priorities of individuals. Thus, the IRGC (2005) has suggested three factors which determine the degree of criticality: 1) Scope – extent of the population and geographic area covered; 2) Magnitude – potential impact or loss (public health, economic, environmental) of supply; 3) and Time-effect – additional damage caused by extended duration of serious impact. 'Risk assessment', in turn, has been defined (Risk assessment and prioritization 2003; see also Moteff 2004, p. 3) as a systematic, analytical process to identify hazards, establish their likelihood, and assess potential severity of a successful attack on some element of the system. It involves the integration of threat, vulnerability, and consequence information. They are necessary for selection and implementation of actions to reduce the risk associated with existing or anticipated threats. From the perspective of deliberate threats, risk assessment should include three basic components: 1) assessment of the threat environment (likelihood for an attack); 2) vulnerability of the system (likelihood that an attack will be successful); 3) and the criticality and magnitude of the possible consequences (impact of a successful attack). It is important that risk assessment is iterative and periodically updated to determine how risks change based on implementation of safeguards and countermeasures. Many models and methodologies have been developed by which threats, vulnerabilities, and risks are integrated and then used to inform the cost effective allocation of resources to reduce those risks.

follows: *Workstream 1* will deal with the strategic aspects of EPCIP and the development of measures horizontally applicable to all Critical Infrastructure Protection (CIP) work; *Workstream 2* will deal with European Critical Infrastructure implemented at a sectoral level; *Workstream 3* will support the Member States in their activities concerning National Critical Infrastructures. The EPCIP Action Plan will be implemented taking into account sector specificities and involving, as appropriate, relevant stakeholders. (Ovilius 2007b)

1.9 REGIONAL MULTILATERALISM IN CRITICAL INFRASTRUCTURE PROTECTION

The question then is, from the perspective of this study, whether a regional level of governance in CIP is needed to intermediate between the national governments and the EPCIP when trying in practice to deal with the extremely complex cross-sectoral and cross-border issues with multiple actors at different levels, especially in a region such as the BSR with strong presence of non-EU countries in the field of cross-border (and European) CI fields.

In a sense, this level already exists, although in a very fragmented form. The BSR is characterised by the existence of a great number of regional intergovernmental, interparliamentary, sub-regional and transnational institutions, networks and programmes, which are partially overlapping in terms of their members and priority areas (Tables 9 and 10).³³ Most or perhaps all of them have a clear CIP-relevance. This fragmented institutional situation reflects the specific historical roots of international cooperation and the respective cooperative solutions in the region.

The roots of fragmentation

All the BSR countries except Russia and Norway – the latter being an EEA country (as is Iceland, too) – are EU Member States, which means that most of the region is regulated by the EU common policies and structures. To fill the gaps, the EU has created some extended cooperation forms, particularly tailored to BSR conditions and addressing also non-Member States. The most notable of these is perhaps the Northern Dimension (ND), which includes not only the EU Member States but other countries in the region as well, and especially Northwest Russia. While the ND was approved by the European Council in 1999, with Action Plans whose final versions were drafted in the European Commission, since 2006 it has become more of an equal cooperation between the Partners, namely the EU, Iceland, Russia, and Norway.³⁴

³³ Information and links to the specifically BSR main organisations are collected under the Baltic Sea Portal (2007) <http://www.balticsea.net/>

³⁴ There were two action plans, 2000-2003 and 2004-2006, which were finalised by the Commission but some regional organisations, most notably the CBSS, participated in drafting these documents. In November 2006 at the Helsinki Summit new basic documents (ND Political Declaration and ND Policy Framework Document) were adopted in the spirit of equality of all the partners (EU, Iceland, Norway, Russia).

Table I—9 Main permanent regional councils, institutions and networks in the BSR.³⁵

Institution		Nature of cooperation	Established	Description
EU-funded regional networks and programmes in the BSR	Northern Dimension	Intergovernmental, transnational	1999	The Northern Dimension policy is a common project of the EU, Iceland, Norway and the Russian Federation. It covers a broad geographic area from the European Arctic and Sub-Arctic areas to the southern shores of the Baltic Sea, including the countries in its vicinity and from North-West Russia in the east to Iceland and Greenland in the west, but focuses increasingly on Northwest Russia.
	INTERREG IV	Cross-border/transnational/Interregional	Current programme period 2007-2013	INTERREG IV consists of three strands: 'A' covering cross-border cooperation; 'B' for transnational projects; 'C' for interregional cooperation. The geographic area it covers in the BSR varies depending on the strands.
CBSS		Intergovernmental	1992	The Council of the Baltic Sea States is an overall political forum for regional intergovernmental cooperation, with several working bodies.
NCM		Intergovernmental	1971	The Nordic Council of Ministers is the forum for Nordic intergovernmental cooperation of most policy areas
BEAC		Intergovernmental	1993	The Barents Euro-Arctic Council is forum for intergovernmental cooperation in the Barents Region.
AC		Intergovernmental/Transnational	1996	The Arctic Council is a high-level forum for cooperation, coordination and interaction between Arctic states, indigenous communities and other Arctic residents.
HELCOM		Intergovernmental	1980	The Baltic Marine Environment Protection Commission (the Helsinki Commission or HELCOM) works to protect the marine environment of the Baltic Sea from all sources of pollution and to ensure safety of navigation.
BASREC		Intergovernmental	1999	The Baltic Sea Region Energy Cooperation supports the development of an effective, efficient and environmentally sound energy market for the BSR.

³⁵ Information and formulations in this table follow closely the respective institutions' self-descriptions in their websites.

Institution	Nature of cooperation	Established	Description
VASAB	Intergovernmental	1992	Vision and Strategies for the Baltic Sea Region 2010 is adopted by the Ministers responsible for Spatial Planning and Development in the BSR of 11 countries in spatial planning and development.
BCM	Intergovernmental	1994	The Baltic Council of Ministers is an institution for facilitating the cooperation between the governments of Estonia, Latvia and Lithuania.
Baltic 21	Intergovernmental, transnational	1996	An Agenda 21 for the Baltic Sea Region is founded on to accelerate the work on sustainable development in the Baltic Sea region. It involves the eleven countries from the Baltic Sea Region, the European Commission and a number of intergovernmental organisations, international financial institutions and international non-governmental networks.
NC	Interparliamentary	1952	The Nordic Council is the forum for Nordic parliamentary cooperation. The members of the Council are members of the national parliaments, who are nominated by their respective political party.
BA	Interparliamentary	1991	The Baltic Assembly promotes cooperation between the parliaments of Estonia, Latvia and Lithuania.
BSPC	Interparliamentary (national/subregional)	1991	The Baltic Sea Parliamentary Conference is the parliamentary forum of the BSR between national and regional parliaments.
BSSSC	Subregional	1993	The Baltic Sea States Subregional Cooperation is a political network for decentralised authorities (subregions) in the BSR.
B7	Subregional	1989	The Baltic Islands Network is a network of the 7 largest islands in the Baltic Sea from 5 different countries.
CPMR-BSC	Subregional	1996	Conference of Peripheral Maritime Regions of Europe defends the regional interests of 155 coastal regions, divided into Member Regions. One of it is the Baltic Sea, where CPMR – Baltic Sea Commission takes care of the regional activities.
UBC	Subregional/transnational	1991	The Union of the Baltic Cities includes members in all ten countries surrounding the Baltic Sea, currently altogether 100 Member Cities, working mostly within issue area specialized commissions
BDF	Transnational	1998	Baltic Development Forum is an independent non-profit networking organisation with members from large companies, major cities, institutional investors and business associations in the BSR.

Table I—10 Membership/participation in regional councils, institutions and networks in the BSR.³⁶

		EU/EC	Denmark	Estonia	Finland	Germany	Iceland	Latvia	Lithuania	Norway	Poland	Russia	Sweden	Other	
EU	ND	x	x	x	x	x	x	x	x	x	x	x	x		Each organization has a number of ‘observers’, ‘special partners’, ‘strategic partners’, some times members outside the region, and so forth, which can be other countries, intergovernmental and interparliamentary organizations, international financial institutions, sub-state and city networks, business networks, academic networks, transnational organizations and NGOs
	INTERREG IV	x	x	x	x	x	x	x	x	x	x	x	x	Belarus	
CBSS		x	x	x	x	x		x	x	x	x	x	x		
NCM			x		x		x			x			x		
AC			x		x		x			x		x	x	USA, Canada	
BEAC		x	x		x		x			x		x	x		
HELCOM		x	x	x	x	x		x	x		x	x	x		
BASREC		x	x	x	x	x	x	x	x	x	x	x	x		
VASAB			x	x	x	x		x	x	x	x	x	x	Belarus	
BCM				x				x	x						
Baltic 21		x	x	x	x	x	x	x	x	x	x	x	x		
NC			x		x		x			x			x		
BA				x				x	x						
BSPC		x	x	x	x	x	x	x	x	x	x	x	x		
BSSSC			x	x	x	x		x	x	x	x	x	x		
B7 Islands			Bornholm	Hiiumaa Saaremaa	Åland	Rügen							Gotland Öland		
CPMR-BSC (regions)			3	3	8			2	1				9		
UBC (cities)			9	15	12	5		8	9	2	13	7	21	(Belarus)	
BDF		The network involves more than 2,500 decision makers from all over the region and beyond.													

³⁶ Membership at the respective level, that is, for instance EU is represented in the BSPC through the European Parliament.

Another territorially extended form of EU-funded cooperation is the INTERREG programme, where in its current form also relevant Northwest Russian regions as well as Belarus are full-fledged eligible members with the help of the EU's European Neighbourhood Policy Instrument (ENPI).³⁷

This situation might be interpreted as one where the EU is enough to coordinate the regional activities even in the BSR. However, there are plenty of non-EU regional cooperation forms, which all are reflecting to real needs and in that sense show the opposite. While some of these institutions have been based on decades-long traditional Nordic cooperation, most of them were created in the aftermath of the end of the Cold War, and aimed at bringing the 'West' and 'East' of the BSR together. Since then, their profile has been developing and changing, and even now there is a kind of confusion and search for new roles of the regional institutions and networks in the midst of growing overlaps and complexity.

The main actors are the four territorially organised intergovernmental councils dealing with several issue areas simultaneously: the Council of the Baltic Sea States (CBSS), Barents Euro-Atlantic Council (BEAC), Arctic Council (AC), and Nordic Council of Ministers (NCM). Some intergovernmental regional cooperation is functionally organised as, for instance, the Helsinki Committee (HELCOM) dealing with marine environment and maritime safety, the Baltic Sea Region Energy Co-operation (BASREC), and Vision and Strategies for the Baltic Sea Region 2010 (VASAB) in the field of spatial planning and development. In some cases these councils or institutions include other than BSR non-EU countries, as in the case of the AC, of which the USA and Canada are members. The Commission of the EU also participates actively in the work of these councils, as a full member as in the case of the CBSS, or as an observer in some other cases. Several other European countries and organizations are usually more or less active observers in the BSR intergovernmental bodies. The different regional organizations tend also to be official observers or strategic partners of each other. The parliamentary level of this regional cooperation is the Baltic Sea Parliamentary Conference, being a forum for national and regional parliaments.

The most integrated and developed regional cooperation forums, both in terms of organisational and financial resources as well as policy programmes, are however founded around traditional Nordic cooperation, such as the NCM and its parliamentary counterpart Nordic Council (NC). Although these organizations have been open to all kinds of cooperation with the 'outsiders' and have signalled this inclusive strategy by establishing information and coordination offices in Northwest Russia and the Baltic States and cooperating closely with a wide range of other actors, they so far have decided not to endanger this very well established cooperation by taking, for instance, the three Baltic States as members of this Nordic 'family'. Thus, Nordic cooperation is that taking place between Denmark, Finland, Iceland, Norway and Sweden.

In any case, this tradition of Nordic cooperation has led to the fact that the three Baltic countries of Estonia, Latvia and Lithuania, have established their own

³⁷ Concerning Russia's participation in regional EU-funded cooperation, the current ENPI/INTERREG IV system for 2007-2013 replaced the rather complicated system of TACIS programme, the former EU funding source for involving Russia, which was difficult to coordinate with the INTERREG priorities and funding.

Baltic counterparts to this type of tense cooperation between the ‘likeminded’. Thus, there exists the Baltic Council of Ministers (BCM) facilitating the cooperation between the governments of Estonia, Latvia and Lithuania, resembling though not coming even close to the NCM in its level of integration and respective organisational resources. Its parliamentary counterpart is the Baltic Assembly (BA).

The BSR countries differ in their level of centralisation or decentralisation, but especially the Nordic countries and Germany have traditionally had a high level regional and local autonomy within the nation states. This tradition of decentralised or rather flexible administrative and political systems compared to hierarchic or centralised systems has been adopted step by step in the three Baltic States and Poland, due to their participation in the BSR cooperation but also through their EU membership. Russia is more centralized and especially international cooperation of its regions has perhaps become more difficult or bureaucratic during the past few years compared to the mid-1990s, but there is still room for regional initiatives and activities, including in cross-border issues. This general situation of importance of regions and other local actors in the BSR has led to the establishment of a number of sub-regional cooperation networks between regions, cities and other non-state actors such as trade unions or business councils. Thus, there are the Baltic Sea States Subregional Co-operation (BSSSC), Union of Baltic States (UPC), so-called B-7 cooperation between the Baltic Sea main islands, Baltic 21 focusing on sustainable development efforts, and many other forms of cooperation beneath the intergovernmental and multilateral levels.

Depending on the exact organization, these institutions’ multilateral work is expressed in many forms. They might be prime minister –level summits and declarations, sectoral minister meetings and decisions, operational Task Forces or high-level Working Groups in different fields, regular meetings of Director Generals of different government agencies, joint comments on EU green or blue papers or other initiatives, conferences and seminars, and more concrete large-scale projects, usually within the framework of the EU-funded programmes such as the INTERREG.

CIP-relevance of regionalism

Most of the regional institutions, networks and programmes have a clear relevance to CIP, and there is a clear need for this cooperation. Evaluating their activities explicitly from the CIP perspective, matching their priority areas, programmes, working groups, projects and so forth with those CI sectors listed in the EPCIP (Table 3 above), we find out that there is a lot going on in this field at all levels and in several institutions simultaneously (Table 11). Just to illustrate, these include such as the ND Environmental Partnership (NDEP) focusing mainly on nuclear waste management, the CBSS Working Group on Nuclear and Radiation Safety, BASREC’s Working Groups in several fields of energy (such as gas), HELCOM’s projects and programmes on ships’ traffic and navigational safety and other marine affairs, BSSSC Working Group on maritime safety, and so forth.

A great part of the regional project cooperation within and between the above mentioned institutions and networks is financed by the INTERREG programme, and many CIP-related issue areas (energy, transport, maritime safety, urban structures etc.) are included in these project activities. However, a specific CIP

perspective is usually missing in the INTERREG priority listings, drafted in the spirit of rather traditional spatial planning; an issue which should given attention by the Commission.

Why would this regional multilateralism be important from the CIP perspective? As discussed above, most of the CI interdependencies are regionally determined in one way or another. The regional particularities and the complexity of the issues at stake make these interdependencies such that it seems not possible to address them and coordinate the relevant efforts only ‘in Brussels’ by the EPCIP structures. For instance, the electricity supply of Finland is directly – and physically – connected to Sweden, Russia, and Estonia; oil transportation goes through the Baltic Sea and a major tanker catastrophe would affect several if not all the coastal countries; geographic proximity easily makes national health problems regional; or banking and financing related activities, as well as those related to ICT services, are in many times taken care by companies which operate in several BSR countries through the same web-based systems.

One particular feature of BSR cooperation is that Russia, or a respective Russian administrative level, is involved as full-fledged partner and member in many cases, like in the CBSS, AI, BEAC, BASREC, VASAB, BSSSC. EU-Russian cooperation does not always provide the necessary – detailed or concrete enough – multilateral framework for cross-border cooperation in the field of CIP in the BSR. At the same time, many threats to the very central fields of CI, such as energy supply, nuclear safety, or transport, are necessarily connected to Russia.

As discussed above, this regional cooperation is active but based on a very fragmented and complex network of actors. While it would be impossible to follow or monitor all of these multi-level simultaneous activities from Brussels, coordination is a real regional challenge as well. The challenge and the necessity of coordination arising from the organizational fragmentation has been a widely discussed theme already a longer time, as there seems to be a considerable overlaps both in terms of geographical area and memberships, as well as activities and issue areas.

As such, no-one suggests the establishment of a hierarchic system. Thus, Mariussen et al. (2000), for instance, have argued that there is a trend during recent debates indicating that the classic mode of hierarchical control between and within international organizations is loosing ground, and that information flows and incentive systems, enabling autonomic operation of the different entities working in the same field is preferred. Cooperation and coordination are emphasized mainly at the level of implementation. Though basically supportive towards this trend, Mariussen et al. list several problems arising from this scheme. 1) Insufficient learning may result from the fact that the same lessons may have to be learned over and over again by different agents; 2) Harmful competition and power struggles can lead to wasted resources and the loss of overall objectives; 3) Avoidance of responsibility can be caused without a clear division of tasks; 4) Opportunism, caused by the unclear structures, may influence the agents to go in wrong directions; 5) Information overload is caused by the autonomous agents’ efforts to coordinate their activities at the grass-root level, resulting in too many meetings; 6) Wrong (investment) decisions can be made because of a lack of

Table I—11 Regional councils, institutions and networks in the BSR from the perspective of the EU definition of the CI sectors.³⁸

		I Energy	II Nuclear industry	III ICT	IV Water	V Food	VI Health	VII Financial	VIII Transport	IX Chemical industry	X Space	XI Research facilities
EU	ND	(x)	x		x	(x)	x		x			
	INTERREG IV	x		x	x				x			
CBSS		x	x				x		x			
NCM		x	x	x	x	x	x	x	x	(x)		(x)
AC					(x)							
BEAC		x	x	x	x	(x)	x		x	(x)		
HELCOM		(x)							x			
BASREC		x	(x)									
VASAB		x			x				x			
BCM		x	(x)		(x)		x		x			
Baltic 21		x	(x)	(x)	x	x	x		x	(x)		
NC		x		(x)					x			
BA		x		x			x		x			
BSPC		(x)			x		x		x			
BSSSC		x					x		x			
B7		x			x				x			
CBMR-BSC		x				(x)			x			
UBC		x		x	(x)		x	(x)	x			
BDF								x	x			

³⁸ This listing is the author's subjective evaluation of the priorities of the councils, networks and institutions on the basis of the information on their respective websites indicating the priority areas, working groups, commissions, projects etc. It makes an effort to match these organisational priorities and activities *only* from the perspective of those CI sectors and sub-sectors, which are defined in the EU context, summarised in Table 3. When expressed as x, this means that there are clearly identified activities, like ongoing or planned working groups and projects. When in brackets (x), this indicates that there were some relevant or related activities identified or direct issue-area linkages.

necessary information and co-ordination, caused by the tendency to cut the overhead costs of the autonomous centres.

All of these notions are the reality in the BSR. Thus, while the region has learned to live with complexity and diversity, and to appreciate it, the issue that an ‘umbrella’ or ‘soft coordinator’ would be needed is still often raised by the institutions themselves. The best candidate for this position would undoubtedly be the CBSS, because of all the regional organizations it is a politically high-level intergovernmental organization covering the widest possible territory, that is, all the 11 BSR countries as well as including the European Commission as a full member; its functional specialisation is not limited to any specific field but can be flexible and widened; and it already today is closely following and monitoring the developments in the most organizations by the virtue of been an observer or strategic partner to them.

From the CIP perspective, the CBSS might well have an overall role of identifying the state-of-the-art in the region, the specific regional CIP challenges that cannot be tackled by the governments or the EU alone, and organize, when necessary, joint initiatives and operational task forces to address these challenges.

1.10 CONCLUSIONS

This study is about critical infrastructure protection in general but has a specific BSR perspective. It opens some perspectives onto the particularities of this specific region from the point of view of critical infrastructure protection. These include specific climate conditions, long distances, in some sectors and between some countries closely integrated economies, still a variety of political and administrative systems and cultures as well as institutional solutions as to international cooperation and integration, and very fragmented and multilayered regional networks.

The BSR countries’ approaches to critical infrastructure protection vary, but at least some of them also share common general trends that are worth noting. There seems to be a trend towards broad definitions, or in some countries even a tradition to that effect, that is, focusing rather on vital or critical societal functions than mere infrastructures. There is also a debate rising about focusing more on resilience than mere protection, an approach which would particularly well match the general societal security approaches in at least the Nordic countries. While terrorism-as-a-priority-threat approach has some support, many BSR countries are fundamentally basing at least their own national strategies on all-hazards approach. The general solutions to the majority of the BSR countries’ political and economic systems seem to suggest a rather balanced public-private partnership model, thus limiting itself to coordination and soft regulation. Concerning the European Union’s efforts to enhance the multilateral approaches in critical infrastructure protection, too far-reaching approach would probably be not accepted by most of the Member States in the region; bottom-up approaches are preferred, although the Member States seem to be prepare to accept some soft legislative regulation and welcome more coordination.

In accordance with the arguments provided by the case studies of this study, it is proposed here that these specific conditions should be reflected in the multilateral critical infrastructure protection strategies in order them to become effective. There is a need for a regional strategy of critical infrastructure protection in the BSR, working as an intermediate level of coordination between the national governments' critical infrastructure protection strategies and the European Programme for Critical Infrastructure Protection. This regional strategy could best be coordinated – in close cooperation and consent with other regional councils and networks – by the Council of the Baltic Sea States, an intergovernmental organization including all the BSR countries as well as the European Commission as full members. This regional strategy should be based on full consensus of the parties, thus leaving strongly contested issues beyond its scope. Its focus should be on regional cross-border critical infrastructures as part of the infrastructures defined by the European Union as European critical infrastructure, as well as address regionally determined vulnerabilities and interdependencies of the national critical infrastructures. This strategy should be sensitive to the national critical infrastructure protection strategies, definitions and specific features of the BSR countries, without complicating the European Union – wide development of common standards and strategies within the European Programme for Critical Infrastructure Protection

CHAPTER II: ELECTRICITY

Jyrki Landstedt
and
Petter Holmström

Emergency Services College of Finland
and
State Provincial Office of Western Finland

2 ELECTRIC POWER SYSTEMS BLACKOUTS AND THE RESCUE SERVICES: THE CASE OF FINLAND

2.1 INTRODUCTION

Modern society is highly dependent on electricity, telecommunications and other services delivered through complex technical systems. A well functioning technical infrastructure is important to everyday life, economic welfare and national security. In an energy intensive society, better functioning is continuously expected from the electric grid. Due to increasing energy dependence, a major blackout in urban areas would virtually paralyse the whole society.

Natural disasters, bad weather, technical failures, human errors, terrorism and acts of war may cause disturbances in the technical infrastructures of society. A common reason for long-lasting and widespread electric power system blackouts is the weather. Examples include storms, blizzards, ice storms, extreme cold weather and floods.

Disturbances caused by a technical failure in electric power systems are often shorter and limited to a smaller area than disturbances caused by weather. Unfortunately, in recent decades, we have seen more frequent, longer lasting and wide spread blackouts caused by technical failures. The primary reason for this is the cascading interruptions that may occur in complex power transmission networks.

Rescue services as ‘first responders’ are responsible for detection, assessment, alerting and dispatching of specialized life support and life safety assets in society. While there is a lot of experience in carrying out risk assessment and response training exercises directed to other organizations in society, relatively little attention has been paid to the potential vulnerability of the rescue services organizations themselves. Failures in critical infrastructures would undoubtedly affect their ability to carry out their duties in a negative way.

This analysis discusses the infrastructure system interdependencies of the rescue services. It focuses on Finland, with some comparison with Sweden where more detailed data is available. Emphasis here is placed on the electric power systems and on steps needed to mitigate the effects of lost critical infrastructure services on the mission capability of the rescue services. Information about how the mission capability is affected by long lasting and widespread blackouts has been collected from experiences learnt from the Janika-and Pyy-storms in Finland and the Gudrun-storm in Sweden.

Major accidents or natural disasters caused by freak weather phenomena usually cause widespread destruction or danger to human life, property or the environment. These so-called dynamic accidents occur unexpectedly and have only local impact at first. However, their effect can continue to expand, unless rapid and efficient rescue activities can be organized. Major accidents require rescue resources from a large area and this may impair the ability to conduct other

rescue efforts during a major accident. Major accidents in Finland are normally caused by human error or technical system malfunctions.

Storm and flood damage, at their worst, cause dam failures and devastate buildings as well as other infrastructures. The most frequent ones are riparian floods which annually inundate large land areas. Statistically, a storm flood is the most probable of these. A rise in sea level may cause damage in coastal cities. Finnish citizens abroad may encounter any possible kind of freak weather phenomenon or act of terrorism.

Major accident preparedness comprises prevention, early detection, efficient rescue activities and inter-authority cooperation. Relevant measures can be improved by planning, counselling and training, legislation and technical solutions. Different actors have various statutory obligations.

Preparedness is improved by maintaining and developing technical systems, such as premises security, fire alarm and extinguishing systems, traffic management, traffic safety, radiation monitoring, chemical measuring systems as well as structural resistance against fire and explosions. Counselling and construction help people in identifying the correct courses of action and in risk avoidance. The consequences of natural disasters can mainly be mitigated through construction regulations and land use planning. In addition, the development of forecasting and alarm systems for freak weather phenomena assists the organizing of rescue activities, the protection of people and property as well as evacuations.

2.2 THE ELECTRIC POWER SYSTEMS

Power production based on several types of fuel and sources is promoted in line with the objectives set by the Finnish Government. Necessary legislative amendments support the preservation of an adequate peak production capacity. The reliability and quality of the electric grid as well as distributors' preparedness for blackouts and repairs are improved. (SSFVS 2006)

An electric power system can be divided into power generation, transmission and distribution, and consumption.

Electricity production³⁹

Hydro power has traditionally covered more than half of the power generation up to 1960, but nowadays only 10 % of the electricity is produced by hydro power.

The first four nuclear power plants were built up in the end of the seventies and in the beginning of the eighties, two units in Loviisa and two units in Olkiluoto. Now a fifth nuclear power plant is being built in Olkiluoto. In 2006, almost 25 % of all electricity was produced by nuclear power.

Normally, about 15-20 % of the electricity is imported. In 2006, the net import accounted for 12.7 TWh (almost 13 %) of which 11.6 TWh was imported from Russia. The balance of Finland's electricity trade with the western countries now showed a small export surplus, because of dryer-than-average years in western neighbours. As a rule, Finland has imported substantial amounts of

³⁹ This section as a whole is based on the information from the Finnish Energy Industries (2007).

electricity from the west. The large net import of electricity can be problematic in the future. If domestic electricity consumption in neighbouring countries – especially in Russia - were to increase rapidly, it could have an effect on the availability and price of electricity in Finland.

Renewable energy sources cover 25% of all energy consumption in Finland; a good result compared to other European countries without large hydro power resources.

As the dependency on electricity is increasing in Finland, the heating systems are also changing. Thirty years ago, 40% of all houses were heated by wood. Today, the number is only about 10%. At the turn of the year 2006, about 655,000 residences - inhabited by about 1.6 million citizens - were heated by electricity (about 18% of the heating market). Nowadays, district heating is the most common heating system in Finland. District heating accounts for about 50% of the total heating market (2.5 million citizens).

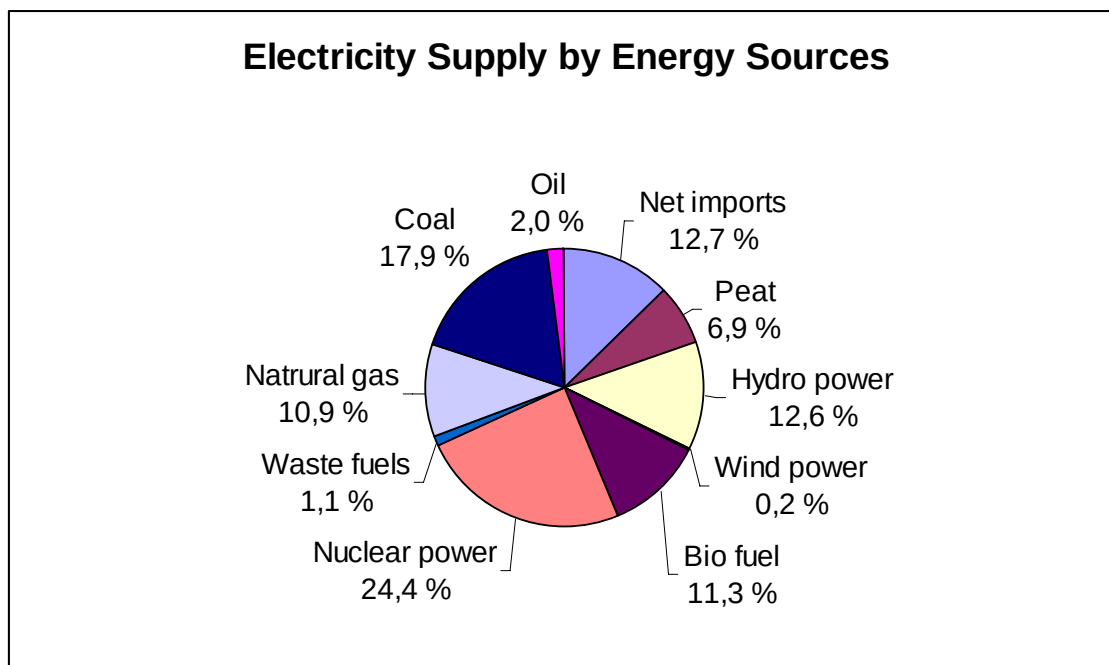


Figure II—1 Electricity supply in Finland year 2006. (Finnish Energy Industry 2007)

District heating is a natural solution for provision of heat and electricity in built-up areas of Finland and can be carried out efficiently in combined heat and power (CHP) plants, which utilize 80–90% of the fuel energy value. When electricity is generated separately, the utilisation rate of fuel energy is a mere 40–50%. Heat and electricity is produced locally using a varied selection of fuels – natural gas, coal, peat, wood and waste wood, or oil – while also taking into account the overall economy and the impact on the environment. Thanks to the efficiency of CHP, emissions to the environment are about 30 % less than in separate heat and electricity generation. Useable heat from industrial production can also be utilised for district heating.

The problem is, however, that there is a very close interdependency between provision of electricity and heat; if the provision of electricity suffers from disturbances, the provision of heat will also get affected, causing additional

problems in the cold winter time. This clearly increases the vulnerability of society.

According to a study made by VTT Technical Research Centre of Finland (Tuomaala 2002), the room temperature of a normal house will decrease from 22°C to 15°C in six hours if the heating system fails and the outdoor temperature is -26°C. In 48 hours, the temperature will drop from 22°C to 0°C. The corresponding temperatures for an energy saving house are 18°C and 10°C, respectively. This gives a time frame for the measures to be taken: bring back electricity and heating, arrange for generators and heaters – or evacuate.

Electricity consumption⁴⁰

In Finland, the consumption of energy and electricity per capita is one of the highest in the world. In the north, winters are cold and dark, and therefore a lot of energy is needed for heating and lighting. Also, the industry in Finland is very energy intensive.

Table II—1 Electricity consumption in Finland and Europe. (Nordel 2004)

Consumption per capita and consumption in Europe Year 2004		
Country	Consumption per capita (kWh)	Consumption (TWh)
Iceland	29400	8,6
Norway	26300	120,1
Finland	16600	86,8
Sweden	16500	146,2
France (2003)	7900	468,2
Denmark	6700	35,7
Germany	6700	554,3
Great Britain	6600	390

In the year 2006, industry and construction used a good 53% of the electricity, households and farms 25 %, and services and public consumption a total of 19 %. A good 3% of electricity was lost during transmission and distribution year 2006. Electric heating across all customer groups accounts for about 10% of the electricity consumption.

Industrial energy demand grew by more than 9.5% in 2006. Electricity consumption of households and agricultural clients grew by 2.3%. Services and public consumption required 3.1% more electricity than the year before.

The variation between seasons is also large. In winter, the consumption of electricity is more than 40% greater than in summer. On the 20th of January 2006, the peak power of total electricity consumption reached an all-time high - 14,860 megawatts. Russia cut electricity export to Finland by several hundreds of megawatts during the most severe frosts and Sweden did the same a little later. However, the demand for electricity in Finland was met.

⁴⁰ This section as a whole is based on the information from the Finnish Energy Industries (2007).

Recent climate events and changes in the climate variability and extremes have received increased attention in the last few years. One of the most obvious consequences forecast by climate models is the raise of the mean temperature. In Finland, this means that the growing season in summer will be four weeks longer than today. Extreme cold seasons will be shorter and less frequent, as the statistical variability of temperature will be larger. The mean temperature will increase and the snow cover decrease.

The need for heating will decrease and therefore electricity consumption has been forecast to increase only 1,2% annually up year 2020 which is less than in recent years (Marttila et al. 2005). Another consequence of the climate change is a small decrease in seasonal variation of energy consumption: in winter, the need of heating energy decreases and in summer, the need of cooling energy increases.

However, it is important to point out that although the average energy consumption decreases, periods of extreme cold or hot weather will become more common. Thus, power companies should have enough reserve capacity to cover the peak load.

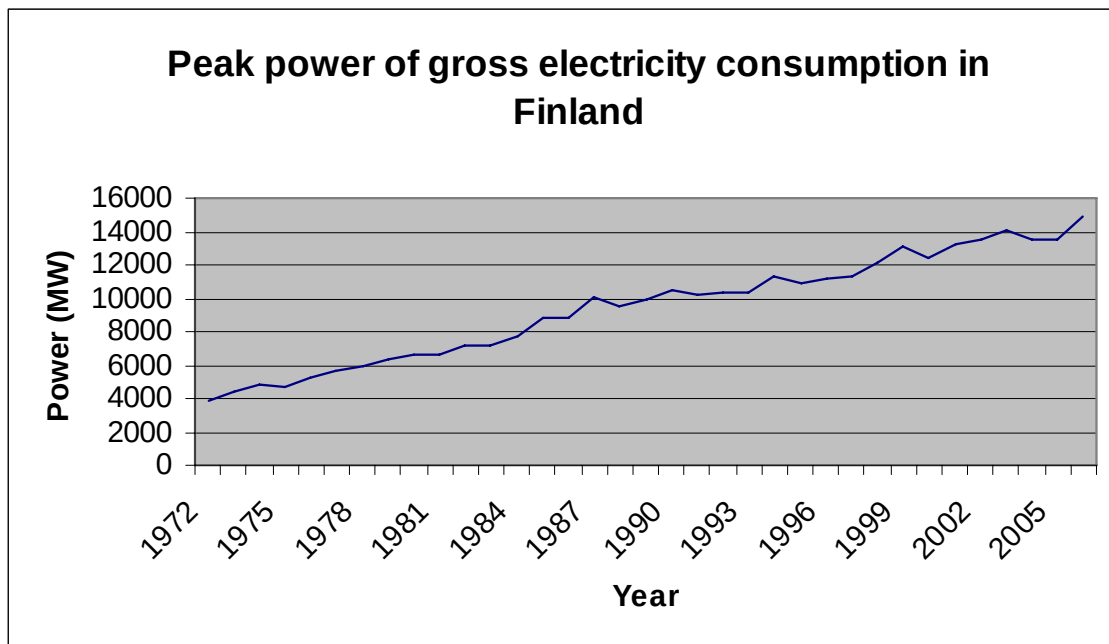


Figure II—2 The peak load trend. (Finnish Energy Industries 2007)

Electric transmission networks⁴¹

The main grid serves power producers and consumers, enabling electricity trade between these throughout Finland and also across Finnish borders. Most of the power consumed in Finland is transmitted through the main grid.

The national transmission grids in the Scandinavian countries are connected together as a Nordic Interconnected Grid. This enables power trading between the countries and facilitates the optimization of power generation within each country.

⁴¹ This section as a whole is based on the information from Fingrid (2007a).

In the north, the Finnish and Swedish transmission grids are connected via an aerial cable. In the south, the Fennoskan marine cable connects Finland and Sweden. In the near future, a new Fennoskan 2 marine cable will be ready for use. The Estlink marine cable links the Finnish and Estonian together. The main connection between the Finnish and Russian transmission networks is 400 kV double lines. Also, there are minor connections near Imatra in South-East Finland and Inari in Lapland. In Utsjoki, Lapland, there is a connection line between Finland and Norway. The most of the electricity used in Åland island between Finland and Sweden comes from Sweden via a marine cable.

The transmission grid (voltage level 400-220 kV) is an interconnected (meshed) network with multiple routes available for the power to reach a certain destination. It carries high electric power over long distances. The sub transmission grid, or regional grid (voltage level 130 – 40 kV), is a radial or locally meshed network connected to the national transmission grid via infeed points.

The high voltage network (over 70 kV) is built using aerial cables, usually with either 400 kV lines and steel towers, or 110 kV lines and wooden poles. Both lines are ensured from fallen trees with a wide right-of-way.

The distribution grid carries electric power from the transmission grid or the sub transmission network to the final consumers. The primary distribution network voltage level is 20 kV or 10 kV. The voltage level for domestic consumers in the low voltage network is 400/230 V.

The medium voltage network (70 kV – 0.5 kV) in rural areas is built using aerial cables with wooden poles, but in cities and built-in areas also underground cables are commonly used. The right-of-way in the medium voltage network is considerably narrower compared to the high voltage network and is therefore more vulnerable to falling trees.

The low voltage network (400/230 V) is a radial network with aerial lines in rural areas and underground cables in cities. Even if the medium voltage and low voltage networks are built as a meshed network, they are normally used as a radial network, which is more economic. However, in case of disturbances, the meshed network can be reconnected and the consequences reduced by ensuring electricity supply from an alternative direction.

The use of different voltage levels in different networks is based on economic optimization and improvement of safety. Different networks are connected to each other via transformer stations where the higher voltage level is transformed to the lower level.

A variety of measuring devices, both at generation plants and spread across the transmission grid, are connected to control centres where they allow operators to monitor the state of the system. By sending electronic commands via telecommunication networks back out, operators can control the settings of the generator plants, reconfigure the grid, and - at least in limited ways - affect its electrical properties. Electricity power system monitoring and grid control are not completely dependent on telecommunications: electricity production, transmission and distribution are working even when telecommunication services are not available. However, monitoring information would not be in real time, which would complicate the control of the power systems.



Figure II—3 The electricity transmission grid in the BSR.

Safeguarding the electric power supply

A focus area, exemplifying the growing dependency on technology, is the security of energy supply. It is a fundamental prerequisite for the systems to function in the information society. Specifically, with regard to electric power supply, sufficient domestic fuel production must be guaranteed, emergency stockpiles of imported fuel must be kept and the reliability of power distribution must be developed by legislative measures, if necessary. As the preparedness obligations for power companies are being considered, international trade regulations as well as the legislation of the European Community must be kept in mind. Prior to issuing the next Finnish *Government Resolution on Securing the Functions Vital to Society*, a more comprehensive report on the options available for improving the security of energy supply is needed.

The production of electricity and heating, the capacity of the electric grid as well as the functioning of technical systems are safeguarded. Electric power supply relies on a functioning Nordic electricity market, an adequate electric grid, dispersed production facilities and multiple sources of energy as well as the proper balance between peak demand and capacity.

Finnish Power Grid Plc (Fingrid) - founded in August 1997 - is responsible for high-voltage power transmission on the national grid, for grid maintenance and grid development. In addition to the grid comprising the 400 kV, 220 kV and 110 kV power lines, the company also owns cross-border lines between Finland and Sweden, Finland and Norway and Finland and Russia. Fingrid also assures the technical functioning of the power system in Finland and contributes to a sufficient quality level of electricity. (Fingrid 2007a)

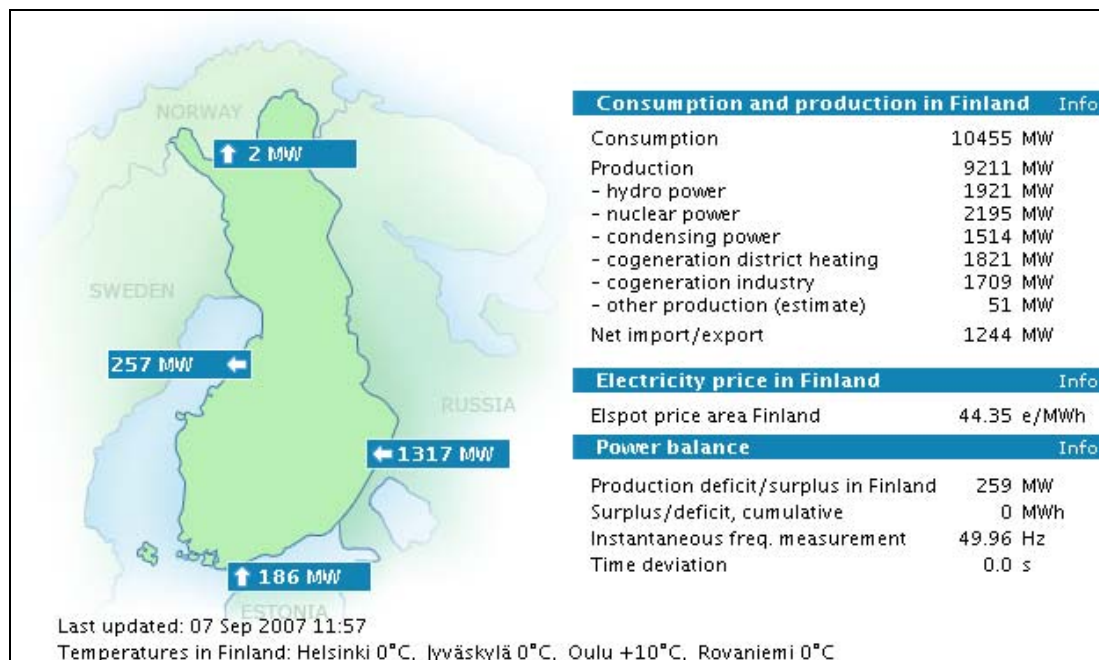


Figure II—4 State of Power System. (Fingrid 2007b)

The Electricity Market Act (386/1995) which entered into force in 1995 opened the Finnish electricity market to competition. At the first stage, only the major electricity users were allowed to invite tenders from electricity suppliers. The

possibilities of small consumers, like households, to invite tenders from electricity suppliers were possible in autumn 1998. In compliance with the Act, the Electricity Market Authority was established to supervise power network operations and to carry out other public tasks. The Electricity Market Act lays down strict requirements for the fairness and impartiality of the company's operations.

The Finnish power system is also operated in accordance with principles agreed upon jointly by the Nordic transmission system operators. The power system must withstand any single fault at all times, without expanding the disturbance. This principle is taken into account in issues such as determination of transmission limits and maintenance of reserves.

Electricity production and consumption must constantly be in balance. Fingrid is also responsible for maintaining a continuous power balance in Finland and for national balance settlement. A three-step procedure is used when the balance between electricity consumption and production is tightening (Fingrid 2007a):

- *Strained power balance:* If production and consumption forecasts show that production and import may not cover the consumption in the Finnish power system during the next few hours, Fingrid will send a notice of strained power balance to balance providers, which produce the electricity. In such a situation, balance providers shall pay particular attention to the planning of their production and consumption and prepare for the situation.
- *Power shortage:* A power shortage is deemed to have occurred when fast disturbance reserves have been activated for balance management purposes. The capability of the power system to resist failures is reduced. During winter, the condensing power plants, within the peak load power arrangement, are kept in a starting readiness of a maximum of 12 hours. The producers are obliged to offer electricity to the market during the peak load period as stipulated by the rules of the system. If the maintenance of the power balance so requires, the plants can be started by Fingrid. The system is financed through separate fees based on the Act. Fingrid is entitled to collect these fees from the users of transmission services in conjunction with fees levied on main grid service and cross-border transmission service.
- *Serious power shortage:* A serious power shortage is deemed to have occurred when all the power reserves are in use and Fingrid has to restrict consumption to secure the function of the power system. Fingrid will contact the local network operators to take necessary actions to restrict loads according to beforehand prepared plans.

The big question in electricity production in the future is how to meet the growing demand of electricity consumption and how to maintain the adequate security supply. If a large severe frost were to hit the Scandinavia, southern Finland and the St Petersburg area at same time, the electricity consumption would most likely have to be restricted in the entire area. This would have an effect on Finland too, because its electricity production is very dependent on electricity import.

2.3 ELECTRIC POWER SYSTEM DISTURBANCES

The majority of the serious electricity blackouts are caused by different weather phenomena, such as storms, snow and ice. Distribution interruptions caused by technical problems are usually restricted to small areas and have a short duration. The power lines in Finland have been designed to withstand normal storms. Interruptions are primarily caused by trees falling over the lines and usually affect distribution networks. The transmission and sub-transmission networks are tree-proof and therefore not vulnerable to the same extent.

Aerial lines are often struck by lightning, in which case short circuits or earth faults may occur. Lines or transformers may also be damaged, sometimes permanently. The underground cables are seldom damaged by lightning; however, if they are, the recovery times are longer compared to damages in the aerial lines. If the power stations or distribution networks are also damaged, the interruptions may affect widespread areas.

During winter, snow may cause power interruptions, mainly by pressing tree branches onto the lines. On rare occasions, snow masses may press entire lines to the ground. No severe problems caused by ice (such as the 1998 ice storm in Canada) have been reported in Finland.

Floods and heavy rainfall may cause disruptions in the underground cable networks, mostly by damaging transformers. Aerial lines are not affected to the same extent.

Subzero temperatures may damage disconnectors, switches or protective fixtures, or even break entire lines. It is important to point out that even shorter power distribution disruptions may have severe consequences to the customers in subzero weather.

Disruptions of non-weather related causes, such as structural or operational errors, are usually short-lived and isolated to a smaller area. However, damages in transmission or sub-transmission network (e.g. due to a broken component) may cause widespread distribution disruptions. Fortunately, these are not very common. The duration and number of electricity blackouts in Finland are constantly low. The reliability of the electricity distribution in 2006 was over 99%.

In 2006, the electricity consumers in Finland had, on average, only a few electricity blackouts whose duration was less than hour. In rural areas, where the electricity grid consists mainly of aerial lines, electricity blackouts occurred more often and were also longer lasting compared to the populated areas and cities. Especially falling trees in the high winds and storms can damage the aerial lines seriously, requiring long lasting repair efforts. In rural areas, the average interruption time due to electricity blackouts was three and a half hours in 2006. In populated areas, the average interruption time was a little above half an hour and in cities about ten minutes. The number of blackouts per consumer in 2006 was 13 in the rural areas, three in the populated areas and only one in the cities. (Finnish Energy Industries, 2007)

The dependency on electricity in modern society is high and will not be reduced in the future. The increase of extreme weather conditions caused by the climate change is a threat to the electricity distribution in the future, and the warmer atmosphere will contain more humidity, increasing the possibilities of heavy rainfall. Consequently, heavy rains with floods, similar to those found in

continental Europe today, may be expected in Finland as well. Many simulation models forecast that the number of deep low-pressures with high winds will increase in the future.

The last strong storms that caused a lot of damage to the forests and serious electricity blackouts hit Finland in 2001. After these two strong storms, called Janika (1.11.2001) and Pyry (15.11.2001), the average duration of the electricity blackout was almost seven hours in rural areas and over four hours in cities.

Storms Pyry and Janika in Finland 2001⁴²

The first of two storms, named Pyry, hit western Finland on the 1st of November 2001. Inland ten minute mean wind speeds of 14 – 18 m/s from north-northwest were measured, with local gusts passing 20 m/s. Although the wind speeds remained below the official storm limit (21 m/s 10 minute mean wind), the damages were big in the Ostrobothnia and Keski-Suomi regions.

The second storm, named Janika, of the same magnitude hit two weeks later, on the 15th of November 2001. This storm did not reach official storm limits either, but still caused even more damage than the previous one, mainly due to short gusts of 30 – 50 m/s. The biggest damages were suffered in the Pirkanmaa, Tavastia and Uusimaa regions.

During both storms, more than 90 000 trees fell over power distribution lines, causing several blackouts. About 800 000 customers were affected by the blackouts, of which 1 600 for more than five days. 30 000 network failures were repaired and 140 km of power lines were rebuilt. The maintenance costs of the electricity companies reached 11 million euros.

More than three million cubic metres of trees were damaged, to a value of the same magnitude as the maintenance costs.

Precautions

A weather forecast was sent out by the Finnish Meteorological Institute in the morning on the 1st of November. As a consequence, the Department for Rescue Services of the Ministry of the Interior urged the state provincial offices of Western Finland and Southern Finland to advise the fire departments to raise their level of preparedness. In addition, the fire departments were advised to investigate the availability of backup power sources. Generators were borrowed from municipalities and other provinces. A significant amount of equipment was also provided by the Finnish Defence Forces.

In general, the precautions taken before ‘Janika’, on the 15th of November, were similar to those taken before ‘Pyry’. The inventory of backup power sources turned out to have significant value during the second storm as well.

Direct Impacts of Power Blackouts

The role of the emergency response centres was significant in receiving emergency calls and dispatching rescue units. During the storms, thousands of emergency calls were received, of which the vast majority concerned requests for clearing assistance due to fallen trees. In addition, some incidents were reported directly to

⁴² This section as a whole is based on the information from Viitanen (2002).

the fire stations. Due to the large number of assignments, the rescue authorities were constantly required to evaluate and prioritize them, in order to prevent duplicate visits to the same location and maintain preparedness for handling urgent emergencies. As the officer in charge could have more than 20 simultaneous requests for assistance to deal with, the line had to be drawn somewhere. Urgent assignments had the highest priority, clearing trees from traffic routes came next. Overall, clearing assignments were carried out only if they caused immediate danger to life or property.

The power lines were mainly cleared by the power companies themselves. If assistance was requested from the fire departments, it was only granted if enough rescue resources were available.

The majority of the rescue assignments during these two storms concerned fallen trees and other debris, damaged roofs, collapsed constructions and drifting boats. The fire departments also delivered generators to high-risk farms and real estate owners. For example, a nursing home for elderly people was assisted in maintaining their heating and lighting in Pylkönmäki.

Communication

During the storms, about 24 000 customers were affected by interruptions in the fixed telephone network, of which the longest lasted for about ten days. The failures were mainly caused by trees over the telephone lines or power shortage in switches due to insufficient backup power.

The mobile telephone network also suffered from interruptions; about 250 000 customers were affected. Although the downtime of the mobile telephone network was significantly smaller compared to the fixed telephone network, some base stations remained out of order for about six days. The interruptions were caused by power shortage in base stations, as the batteries were not dimensioned for blackouts of this magnitude. Backup power generators were either not available at all, or they could only be delivered to the most important base stations. Another problem that arose was the inability for the customers to recharge the batteries in their mobile phones.

In Finland all safety and security authorities use a common nation-wide authority radio network called VIRVE, which is based on the TETRA (Terrestrial Trunk Radio) standard.

At the time of the 'Pyy' and 'Janika' storms, the transition from the old analogue radio systems to TETRA was in progress; thus all vehicles were also equipped with the old radio terminals.

During the storms, tens of VIRVE base stations failed, resulting in a complete loss of the network services in some areas. This again endangered or prevented dispatching of units, intra-organizational coordination and interoperability between authorities.

The primary reasons for the failure were that either the base stations themselves or the routing systems between the base stations and the network ran out of power. Most base stations were equipped with backup batteries, but with insufficient capacity.

Fortunately, the old radio networks were still operational and hence allowed the rescue units to carry out their duties.

Indirect Impacts of Power Blackouts

The local authorities in the municipalities had several difficulties in maintaining their public services during the blackouts. The water supply and sewerage are dependent on electricity, as is heating. Therefore, normal activities in buildings need special attention and preparedness during blackouts. Fortunately, the outside temperature was mild in November 2001; extreme cold weather would have made the situation much worse. This time, rescue authorities only needed to update the evacuation plans and raise the preparedness to evacuate vulnerable buildings like nursing homes for elderly people and health care centres without alternative heating or backup power. No evacuation plans had to be put into action.

Preparedness planning is obligatory for all public authorities on all levels (the government, the provinces and the municipalities). Some key companies in the private sector, such as power companies and telephone operators, are also obliged to maintain preparedness plans. Despite this, however, experiences from the storms in 2001 showed defects in the preparedness for longer power blackouts.

Experiences and Plans of Improvement

Overall, the fire departments managed all right during the storms. The available resources were sufficient, mainly due to the contribution made by the voluntary fire departments. In the aftermath, suggested areas requiring additional development included improved anticipation of weather-related assignments, registries of available (or missing) power supplies, uninterrupted support for recharging radio batteries, secured fuel distribution and improved wood cutting skills for the fire fighters. Better interoperability between the power companies and the rescue authorities was also requested. Emergency services organizations must equip themselves and train for operations during power blackouts.

Electricity companies and telephone operators should improve their infrastructure and preparedness to respond more quickly to weather related disturbances. The private sector, which is operating in the open market under hard competition, finds it difficult to invest more in preparedness than is economically justified. In the case of power blackouts, rapid, well-timed and precise information to the public about the size and duration of the blackout is essential. Improvements will be required in several areas in the future.

The responsibility of the electricity consumers was also highlighted. They have to prepare themselves even better for power blackouts, according to their demands and risks. The more central role the consumer has in providing vital services for society, the more important adequate preparedness planning and quick response is.

Storm Gudrun in Sweden 2005⁴³

The southern parts of Sweden were hit by a powerful storm with hurricane winds between the 8th and 9th of January 2005. The storm reached its climax between 18:00 and 22:00 at the 8th of January and was named 'Gudrun' by the Norwegian Meteorological Institute. The power distribution- and telecommunication

⁴³ This section as a whole is based on the information from the Swedish Rescue Services Agency (2005).

networks, roads, railroads and buildings suffered major damage, with long-term consequences for the people living in the affected areas. Immediate repair efforts were compromised by blocked roads and the danger of falling trees. Roughly 870 000 customers were affected by the blackout.

This case study will concentrate on the effects the storm had on the emergency services in the area, with emphasis on power blackouts.

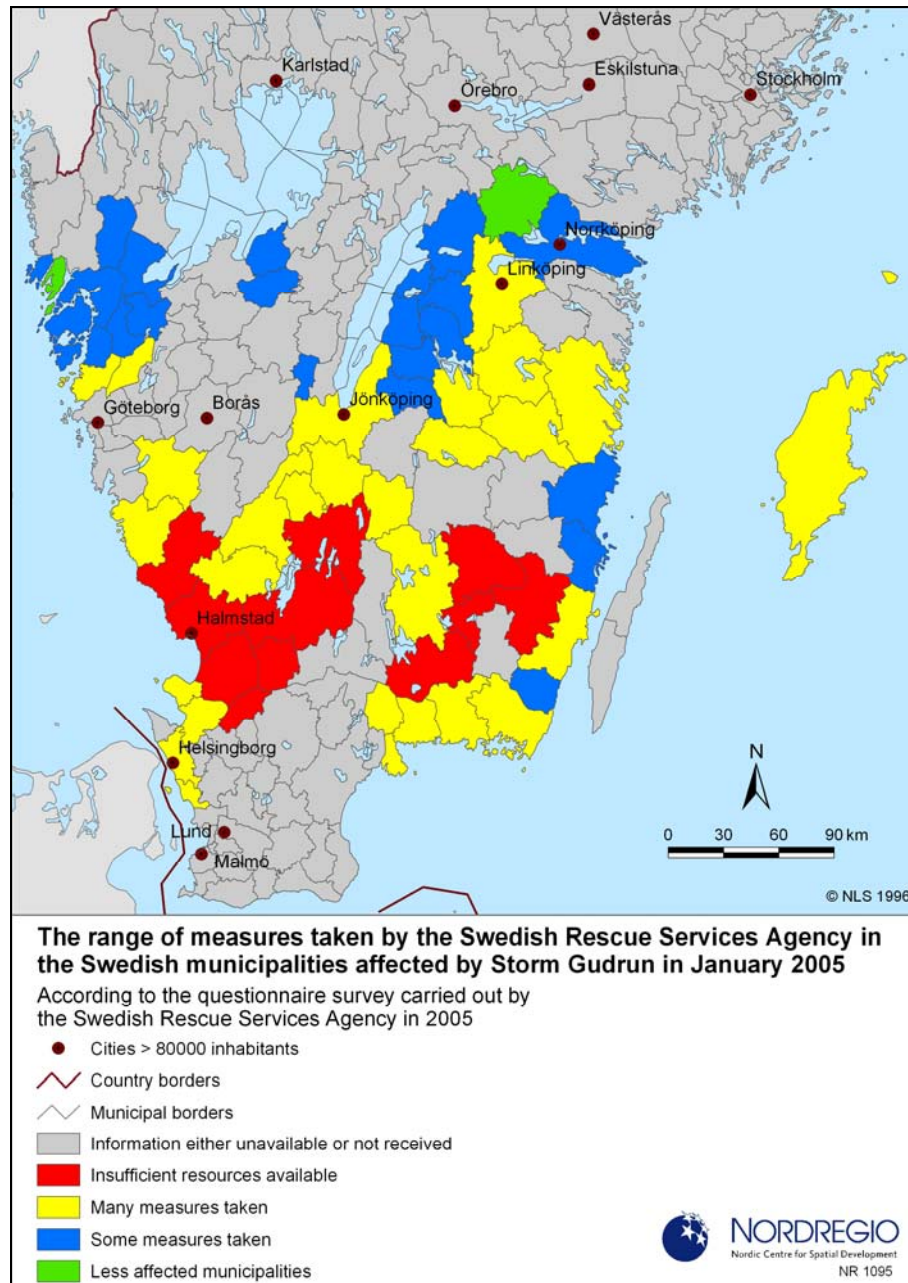


Figure II—5 Measures taken by Rescue Services. (Swedish Rescue Services Agency 2005)

Precautions

On Friday the 7th of January, a weather warning was sent out by the Swedish Meteorological and Hydrological Institute at 23:18. The warning was passed to the

fire departments by SOS Alarm, the Swedish emergency response centre. The majority of the departments immediately raised their states of alert. As the wind kept rising, the state of alert was further increased; additional personnel were called in. No further precautions were taken. However, during the night between Saturday and Sunday, many rescue units were pulled back due to the increasing risk of falling trees.

Direct Impacts of Power Blackouts

The direct impacts on the emergency services due to power blackouts could have been significantly worse. The larger population centres (mostly cities) had functional power distribution during the storm and hence, larger command- and coordination centres remained operational.

Some fire stations with integrated command centres lacked backup power systems (such as generators). Fortunately, these stations were mostly located in cities and were therefore not affected during this particular event. However, this poses a severe threat to the overall robustness of society and will need to be addressed in the near future.

Many part-time fire stations in the country side also lacked backup power systems and were hence affected by the blackouts. This had a negative impact on the fire stations' role as communication- and information centres when all other means of communication were out of order. At some fire stations, the only working communication systems were the vehicle radios. Recharging of portable radio devices was impossible.

The operational abilities of the stations were also affected due to loss of heating. Fortunately, the weather conditions after the storm were favourable; heavy snowfall and low temperatures would have rendered many fire stations completely use-less.

The prioritizing of backup power equipment was handled by the county administration boards in some of the affected areas and by the municipalities themselves in others.

The biggest impacts were due to communication problems, although the communication between units and command centres was working satisfactorily in most areas, for most of the time. This aspect will be discussed in more detail in the following section.

Communication

In some areas lack of communication was considered a far more serious problem than power blackouts. In the case of Gudrun, communication disruptions were mainly caused by either direct damage on phone lines and base stations (fallen trees, etc.) or by power shortage. Some critical base stations were equipped with backup power systems, but in many cases they were not dimensioned for a blackout of this extent. Batteries ran out of power and generators ran out of fuel. Refilling was impossible, as the affected stations could not be reached due to debris and danger of falling trees. Some stolen generators were also reported.

During the storm, authorities (such as fire services, ambulance and police) used 80 MHz analogue radio communications. The operational status of the system varied between areas; in some areas it was fully functional - in others completely

out of order. Again, the primary reasons for communication failure were lack of power for communication base stations.

Both the mobile- and the fixed telephone networks suffered from disturbances; at one point roughly 300 000 customers were lacking means of working telecommunication. Some of the radio communication stations used by fire services and SOS Alarm were also damaged.

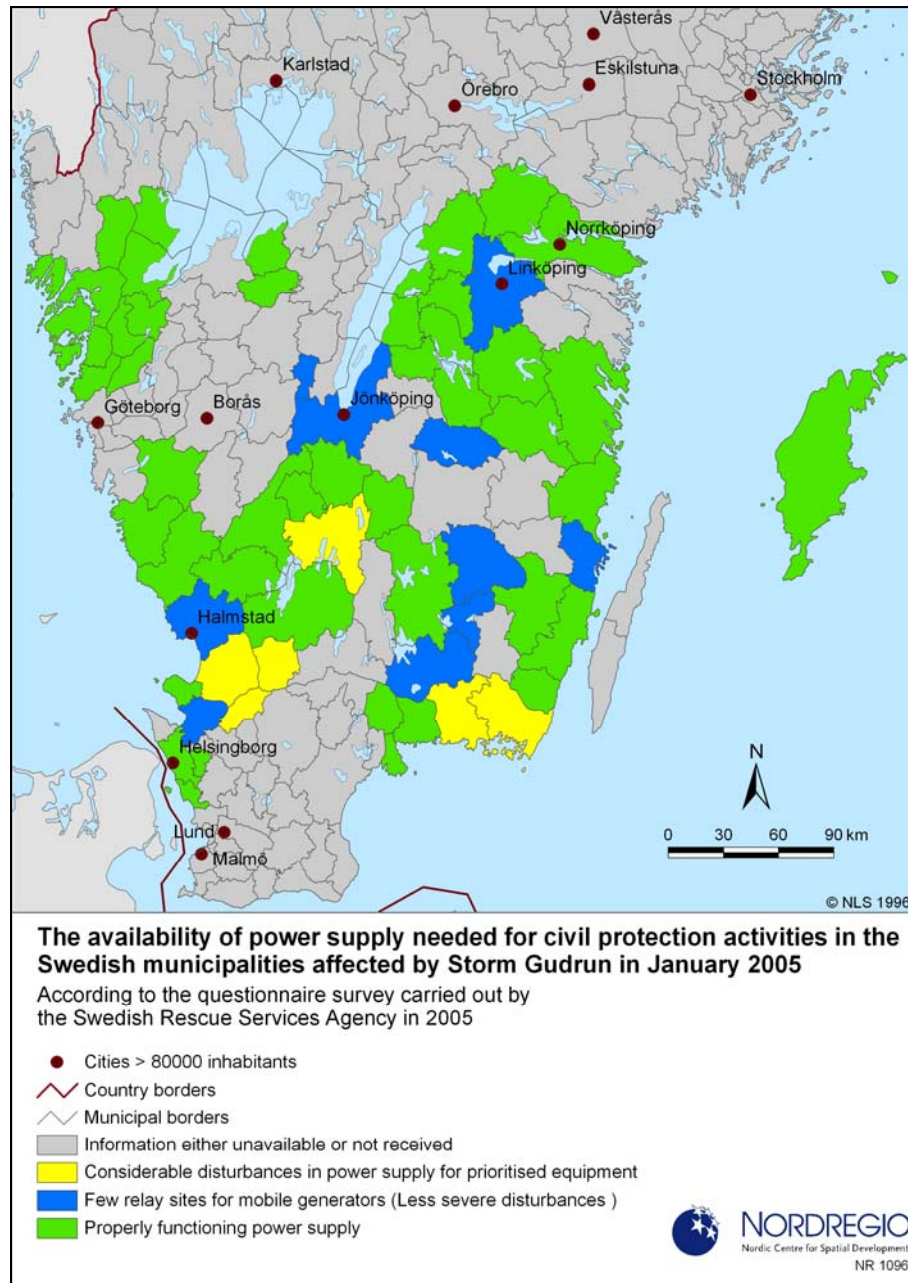


Figure II—6 The civil protection infrastructure and the power supply network affected. (Swedish Rescue Services Agency 2005)

This had the following effects on the emergency services:

- Lack of interoperability between rescue units and other actors, such as the power and telephone -companies.

- Local communication problems between SOS Alarm and the rescue units.
- Problems calling in additional personnel and alerting rescue units.
- Problems for the public to report emergencies to SOS Alarm.

There were also some problems concerning roaming between different mobile operators.

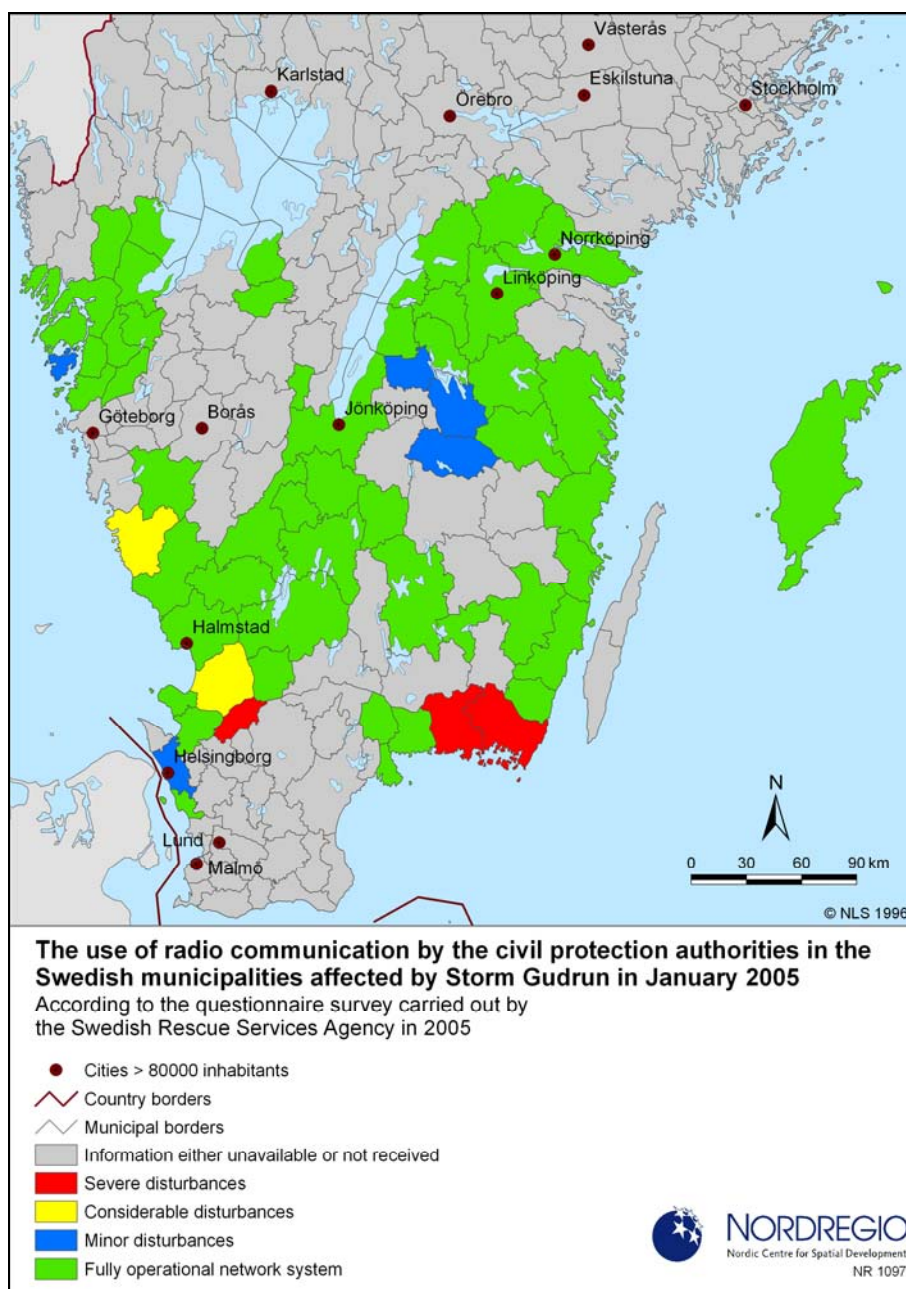


Figure II—7 The civil protection and radio communication affected. (Swedish Rescue Services Agency 2005)

As the emergency number 112 was unreachable in several areas, local fire departments had to set up custom solutions in order to alert rescue units. Many incidents were also reported directly to the fire departments.

Two days after the incident, more than 90% of the mobile network was operational. In comparison, several customers lacked fixed phone communications for several weeks.

Overall, all fire departments who had planned for communication breakdowns, and had redundant- and/or backup equipment in place, managed quite all right.

Indirect Impacts of Power Blackouts

Elderly or disabled people are especially vulnerable to blackouts. Several nursing homes were affected by the blackout and evacuations were considered but never executed. Some municipalities combined their inhabitant registries with Geographic Information Systems (GIS) in order to locate and reach elderly people living on their own. There are no accounts of whether the fire departments were directly involved with the evacuation of people, although it is highly likely.

Some fire stations equipped with backup power acted as ‘warm cottages’ for the public, i.e. a place where people could warm themselves and get the latest information about what is going on. Schools and community centres were also used for this purpose. Some areas experienced water distribution problems, which could have required measures from the emergency services, had they been prolonged.

The availability of fuel for vehicles and equipment was not affected, mainly due to the fact that larger population areas were not suffering from power blackout. However, there were problems with the distribution of fuel to backup power generators, as previously mentioned. These were due to lack of organization and logistics, and blocked roads.

Experiences and Plans of Improvement

The biggest need for improvement is the development of independent emergency supplies. When everything else fails, the emergency services should be prepared and equipped to continue their operations independently.

The role of the part-time fire stations during exceptional situations turned out to be significant; hence many fire stations are now being equipped with backup power facilities. Most of the command centres are also resistant to power blackouts nowadays.

The radio communication problems between authorities will be solved by the introduction of the digital TETRA-based RAKEL network. Important cooperation partners from the third sector (power and telephone companies) are also going to be a part of this network, thus eliminating the interoperability problems. Additional resources have been allocated to make the base stations even more robust; all stations will have backup batteries and many will be equipped with automatic power generators designed for longer blackouts.

Emergency dispatching relies heavily on the telephone communication networks. Therefore measures are to be taken to improve the reliability of these as well. If the systems were to fail in spite of the precautions, backup systems for reporting incidents and alerting rescue units should be ready to put into action with little or no delay.

Concerning the reliability of information systems, there were some problems due to the usage of centralized servers. To reduce vulnerability in situations like

these, systems should be distributed in order to avoid single points of failure. In addition, the use of redundant communication links, such as fibre or satellite, is to improve the reliability even further.

During the storm, the emergency services did not only experience problems of a technical nature - some areas also experienced problems with coordination and organization. On one occasion the fire station was required to house the local municipality coordination group, which had a negative impact on the fire department's own coordination abilities. Basically, all fire departments that had working command and coordination centres did not experience any management problems.

An urging need for GIS and Decision Support applications was discovered during the storm and are currently under development.

Reflections

It is apparent that the consequences of the Gudrun storm in Sweden were far more serious than those of the Pyry and Janika storms in Finland. Nevertheless, there are several similarities as well as a few differences that are worth noting.

During Gudrun, the emergency services themselves were more directly affected by the power blackouts than during Pyry and Janika. The primary reason for this was simply the fact that the blackouts during Gudrun covered a wider area and lasted longer. If a storm of the same magnitude hit Finland, the Finnish authorities would have to deal with the same kinds of problems. This highlights the importance of independent emergency supplies for the emergency services organizations. Actions to improve the preparedness inside the organizations themselves have already been taken, both in Finland and in Sweden.

Both the Finnish and the Swedish authorities suffered from communication problems. As has been noted earlier, the Finnish TETRA-based radio network VIRVE – which had recently become operational – failed during the storms. In Sweden, a similar network named RAKEL is currently being built. Due to the experiences from Gudrun, additional resources have been allocated to make the RAKEL base stations even more robust in order to ensure full operation even during exceptional circumstances. Although the Finnish VIRVE-network has been significantly improved since the storms in November 2001, there is no publicly available information about its robustness and coverage during power blackouts.

The importance of securing vulnerable institutions in society during exceptional weather circumstances became apparent during both Gudrun and Pyry/Janika. After only a few hours of blackout, the situation may become serious, requiring immediate action by the emergency services to save lives. The distribution of drinking water and the risk of contamination must also be taken into account during prolonged blackouts.

As has been noted in the case studies, there can never be too much interoperability and cooperation between the organizations involved, no matter whether they are rescue service organizations or companies from the private sector. This does not only apply to exceptional circumstances, it should be a natural part of the everyday activities.

The rescue services themselves are becoming more and more dependent on information systems. Decision support and incident follow-up systems are being developed in both Sweden and Finland. These systems should be designed in such

a way, that they remain at least partly operational when the normal power and communication systems fail. The sharing of experiences and ideas across nation borders becomes an important factor.

2.4 BETTER PREPAREDNESS

After Pory- and Janika-storms MTI appointed Director General Jarl Forsten to make an account to how to develop electricity networks and improve their reliability. One recommendation in Reliability of Electricity Networks -report (Forsten and Lehtonen 2001) was trying to achieve the six hour maximum interruption time in electricity blackouts. The electricity companies can choose the best ways to reach the target, but it would take a long time, because the electricity networks and its components are long lasting investments, which are renewed usually after twenty or thirty years. It is also important to develop new methods to analyse reliability of the electricity networks and improvement actions, so that forthcoming investments can be made efficiently.

Another recommendation in Reliability of Electricity Networks -report touched the compensation, which is paid to the customers due the electricity blackout. The compensation should be based on the real economical costs, which is caused by the electricity blackouts to the customers, but unfortunately this information is not available. The compensation cost is also important to electricity companies, when they are planning their future investments to the electricity networks or the recruitment of maintenance personnel to speed up repairs. It seems that the present compensation model, where maximum compensation is 700 euros, is not working as it should, because the investments in the reliability of electricity networks or the fast maintenance has not been sufficient as we saw during Pory- and Janika-storms.

Reliability of Electricity Networks -report also highlighted the meaning of the co-operation between authorities during the prolonged electricity blackout and precise and fast information to the public about the area, reason and estimated duration of electricity blackout.

Soon after the Reliability of Electricity Networks -report started Lappeenranta University of Technology (LUT) and Tampere University of Technology (TUT) a research on how to develop electricity networks and improve their reliability (Partanen et al. 2006). In this research the maximum interruption times, average interruption times and number of interruptions acted as reliability indicators. These were then compared to the investment, maintenance and compensation costs.

The consequences of widespread and long-lasting electricity blackouts can be reduced by improving the electricity network structure or speeding up the maintenance. As improving the network structure is expensive, a reasonable trade-off between network investments and maintenance costs is required. How large an electricity blackout is it reasonable to be prepared for and what is the acceptable maximum down time?

Traditional way to classify electricity blackouts according to SFS-EN 50160 standard is to divide them in three categories:

- long interruptions, which are more than three minutes
- short interruptions, which are less than three minutes
- voltage fluctuation

This classification method is very technical and technology orientated – the CIP point of view – and does not pay any attention to consequences and resilience. The first time in this research definition of extreme long electricity interruption (lasts more than 12 hours) was introduced. Despite very good statistical information of electricity blackouts, this type of data of extreme long lasting interruptions was not available in large extent, and therefore historical data from the three previous storms - Unto (July 5, 2002), Pyry (November 1, 2001) and Janika (November 15, 2001) - was used to build up a mathematical model for the simulations.

Storm Classifications

Storms are classified in three different categories according the maximum interruption time and the number of affected customers. A mathematical function has been derived from the statistical information, giving the number of affected customers as a function of the interruption time.

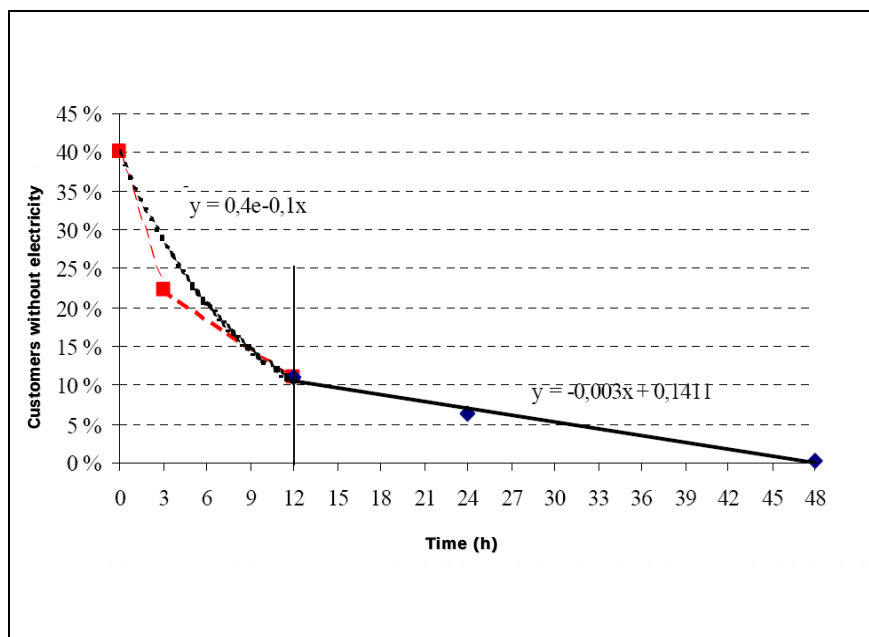


Figure II—8 Customers without electricity in class I major storm. (Partanen et al. 2006)⁴⁴

This is very useful information also for the rescue services for blackout analysis and preparations.

A **class I major storm** is a disturbance that leaves customers without power for a maximum of two days, given the current network structure and available resources. The affected area is normally relatively small and thus the number of

⁴⁴ Mathematical model is fitted to the statistical information on Pyry and Janika storms from Suur-Savon Sähkö electricity company's information system. Actual percentage of customers in coloured points and fitted mathematical function in black.

powerless customers may vary locally from all to none. According to a model, roughly 40 % of the customers in the area will be powerless at the zero hour (the time when the number of powerless customers no longer increases). After 12 hours, the percentage has dropped to 10 %. In 48 hours, all customers have gotten their power back.

A big impact on the time of recovery is the amount of required clearing (fallen trees and other debris) preceding the actual repairing actions. The number and severity of the damages as well as the number of available repair personnel also affect the recovery time.

The assumed rate of occurrence of a storm corresponding to a class I major storm is once every five years.

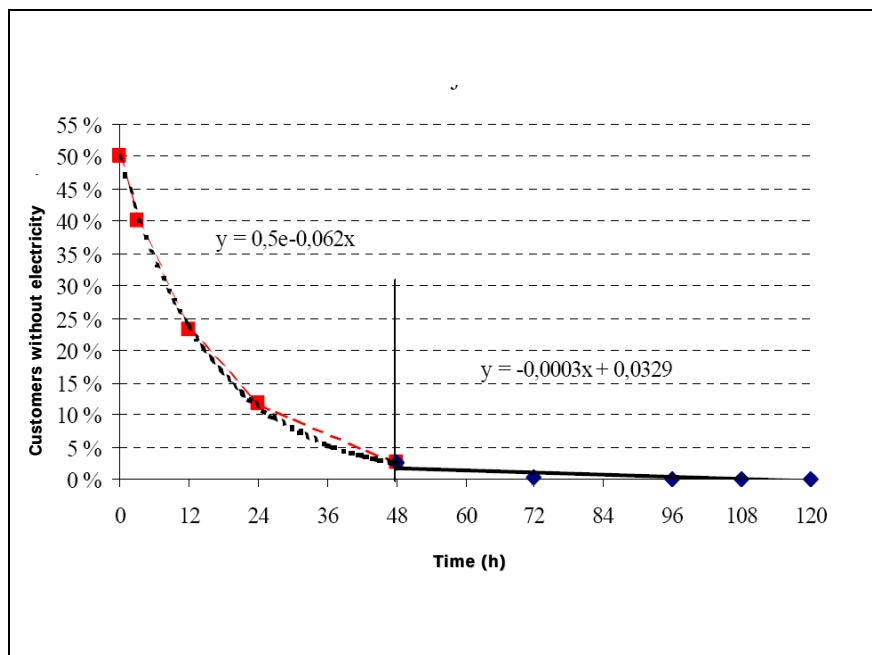


Figure II—9 Customers without electricity in class II major storm. (Partanen et al. 2006)⁴⁵

A **class II major storm** is a disturbance that leaves customers without power for a maximum of five days, given the current network structure and available resources. The affected area normally covers the entire network of the power distribution company and there is little local variation. The only exception is the customers connected to the ground cable networks in cities and population centres; they are normally not affected. According to a model roughly 50 % of the customers will be powerless at the zero hour. After 12 hours, the percentage has dropped to 23 %. Within a day, roughly 90 % of the customers will have their power back; however, it may take as long as 120 hours before all customers have been reconnected. In addition to the class I impacts, the recovery time is mainly affected by three factors:

⁴⁵ Mathematical model is fitted to the statistical information on Unto -storm from Suur-Savon Sähkö electricity company's information system. Actual percentage of customers in coloured points and fitted function in black

- The network suffers severe damages that take time to repair.
- Several repair actions are normally required on the same location due to multiple damages that affect the network independently of each other.
- There are many minor damages spread out over a large area; however only affecting a small number of customers. These are normally the last damages to be repaired.

The assumed rate of occurrence of a storm corresponding to a class II major storm is once every twenty years.

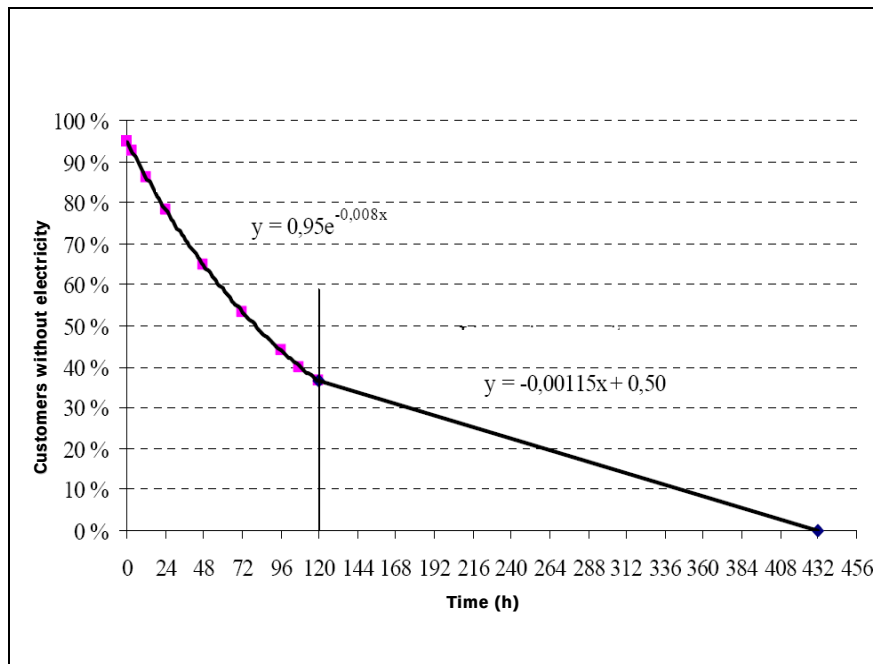


Figure II—10 *Customers without electricity in class III major storm.*
(Partanen et al. 2006)⁴⁶

A **class III major storm** is a disturbance that leaves customers without power for as long as 18 days (2.5 weeks). The affected area may be as large as the entire country, with severe damages on the inter-regional distribution networks, causing blackouts in cities and population centres as well. It is estimated that as many as 95 % of the customers may lose their power before any repair actions can be taken. According to a model more than 50 % will still be powerless three days after the zero hour. After two weeks, 90 % will have their power back.

Storms of class III require a full mobilization of all available personnel. Reinforcements may have to be flown in from the neighbouring countries. The time of recovery is not only affected by the huge number of damages; the rate at which vendors are able to deliver replacement components becomes an important factor.

The assumed rate of occurrence of a storm corresponding to a class III major storm is once a century.

⁴⁶ Mathematical model is only theoretical without statistical background, but if we compare this mathematical model to information from Gudrun-storm, we can notice that the scale is right.

More reliable electric power systems

The current goal is to reduce the recovery time to six hours, even during exceptional circumstances. The current network structure does not support this, as noted earlier.

There are several ways of reducing the interruption time following major storms. The most efficient one is to replace the aerial lines with underground cables, to some extent. This makes the network less vulnerable to most weather phenomena; however, as it has been pointed out earlier in the text, it also makes repairing of damages significantly slower. Class I and II storms do not require the entire network to be replaced, class III on the other hand, does.

Another way of reducing interruption time is by increasing the service personnel. This is a possible solution when dealing with class I storms and to some extent when dealing with class II. However, for class III storms this is not a viable option.

There are also smaller and less expensive ways of improving the power delivery safety. Non-tree-proof wire paths can be improved by cutting all the branches on the inside of the path, forcing the trees to fall away from the path due to e.g. heavy snow masses.

Aerial lines due for renewal should whenever possible be moved from the forests to the sides of the roads. This reduces the risk of the lines being damaged by falling trees and makes it easier for service personnel to reach the damaged spots.

Regardless of all investments in electricity networks and their better reliability continuous electricity supply cannot be guaranteed. If production or other activities need continuous electricity supply, must the customer himself take the actions to secure continuous electricity supply?

Better resilience

Even if the primary point of view of this research was electricity network – critical infrastructure – protection, in the conclusion of the research, there are many elements of improving critical infrastructure resilience (CIR)⁴⁷ like having ready-made plans of how and when personnel should be called in or put in stand-by, keeping maps up to date, following weather forecasts, making deals with third parties for providing spare parts and additional equipment, cooperation with the emergency services, etc. The down time can be significantly reduced by increasing preparedness.

The storm classification and the mathematical model in each category also give a good solid foundation to build up a common knowledge on extreme long electricity blackouts to all parties involved. In the future the information from building information system and information from electricity network simulation model should be combined and so we will have more detailed information what consequences possible extreme long electricity blackout have on activities in different type of buildings. This way we can find out vulnerable activities, such as telecommunication nodes, waterworks, and sewage farms or vulnerable groups in buildings such as hospitals, nursing homes for older people, schools, day-care

⁴⁷ See the discussion on resilience or CIR in Chapter I: Introduction 1.5.

centres etc. This enables better preparedness planning so that electricity companies can focus their repair activities correctly and better preparedness planning with better situation awareness is also the key to successful rescue operations.

In order to achieve better resilience, even the role of the general public is an important factor; it is not the concern of some professional elite alone. Preparedness is to be maintained on all levels, from the common citizen on the street to governmental departments. For example, a home supply of emergency food, drinking water, flash lights, batteries and blankets, etc. is of great significance during a disturbance situation such as a prolonged power blackout.

The emergency services form an important part of critical infrastructure resilience, as they normally are the first ones to respond when a disturbance or accident occurs. However, it is important to note that the emergency services themselves form a kind of CI, vulnerable to disturbances. Therefore, emergency service organizations should have their own emergency contingency plans, enabling them to function efficiently even during exceptional circumstances when resources are limited.

CHAPTER III: INFORMATION AND COMMUNICATION TECHNOLOGY

Krisztina Cziner, Edward Mutafungwa,
Jan Lucenius and Risto Järvinen

Helsinki University of Technology
Communications Laboratory

3 CRITICAL INFORMATION INFRASTRUCTURE PROTECTION IN THE BALTIC SEA REGION: THE CASE OF TETRA

3.1 PROBLEM DESCRIPTION AND DEFINITION

Introduction

The development of information culture can be traced from the oral or spoken word, to tangible manuscripts and print, and eventually to the soft or electronic information that is prevalent today. Electronic information is typically in audio or voice, alphanumeric (that is, data) or video formats. The ability to access, capture, store, process and distribute electronic information rapidly is now the key to the successful operation of both public and private organizations operating in any one of a range of sectors shown in Figure 1. As such, these capabilities are now strongly correlated to national security, the raising of the standard of living and sustenance of technology-driven knowledge-based economies. Therefore, the availability of reliable, secure, affordable and flexible information and communications technology (ICT) solutions is considered by many to be a mainstay of every country's national interests.

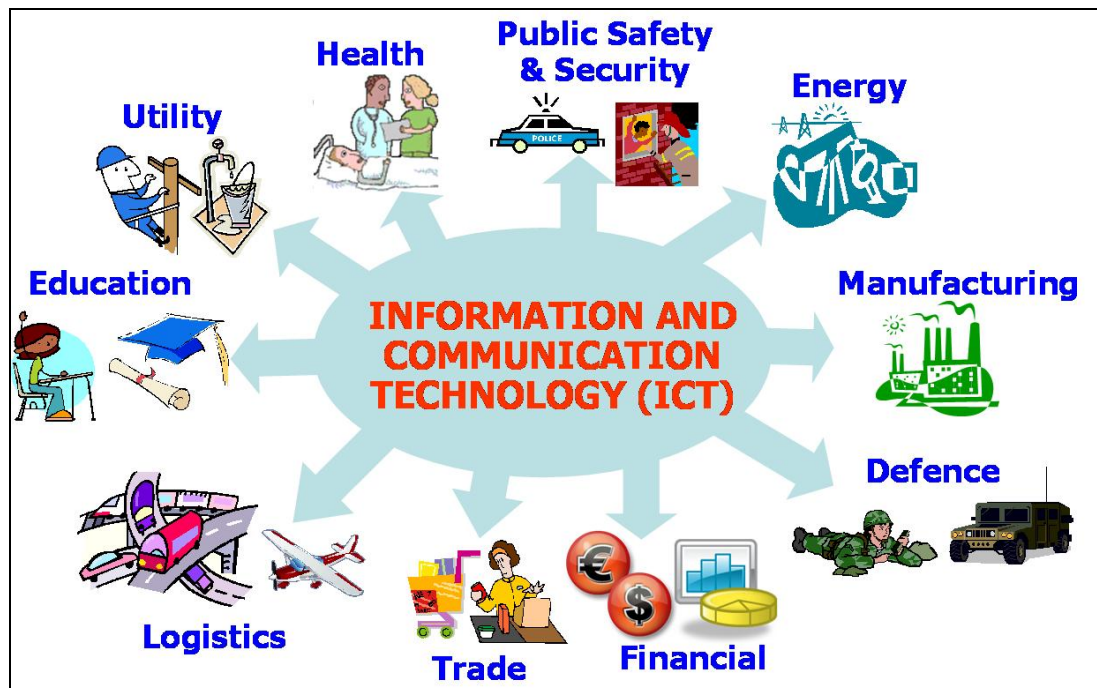


Figure III—1 Sectors whose operations are strongly dependent on ICT.

The ever increasing dependence on ICT solutions represents a crucial need, which can only be met by underlying ICT systems that function according to expectations, whenever and wherever they are called upon. A subset of these ICT systems has come to be known as critical information infrastructure (CII). Although the definition of CII may differ somewhat from country to country (Abele-Wigert and Dunn 2006), the common perception of CII is of them being ICT systems that are critical infrastructures in themselves or that are essential for the operation of critical infrastructure (CI) (Commission 2005b). The likelihood of a protected CII continuing to function in the presence of failures and ensuing disruptions is relatively higher than an equivalent CII without protection. This basic premise is the foundation for critical information infrastructure protection (CIIP) (Dunn and Mauer 2006). It has to be noted, though, that the designation of what is a (or are) CII out of the many existing ICT systems is never a straightforward task (Dunn 2006). This task is further complicated by the interconnectivity between the different ICT systems and their inhibited reach, enabled by the migration from isolated purpose-built systems to flexible converged systems based on the Internet's borderless malleable architecture.

The rest of this section expounds on the general threats prevalent in most ICT systems, especially those considered to be CII. Section 3.2 focuses on a particular CIIP case study with illustrative examples, while Section 3.3 presents a multidimensional strategy for protection against the threats highlighted in the first two sections. The report's conclusions and way forward are then presented in Section 3.4. Throughout the report special emphasis will be placed on analyzing CIIP from a Baltic Sea Region (BSR) perspective.

Overview of threats and interrelated concepts

The concept of information security *threats* is closely interrelated to the concepts of *security*, *attacks* and *vulnerability*:

Table III—1 Two alternative definitions on information security, threat, attack and vulnerability.

Concepts	Definition according to ITU-T 1991	Definition according to IETF RFC 2828
Security	A term used in the sense of minimizing the vulnerabilities of assets and resources	Measures taken to protect a system, or the condition of a system that results from the establishment and maintenance of measures to protect the system. Alternatively, defined as the condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.
Threat	A potential violation of security	A potential for the violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability
Attack	An intentional threat that has been realized	An assault on system security that derives from an intelligent threat. That is, an act that is a deliberate attempt to evade security services and violate the security policy of a system
Vulnerability	Any weakness that could be exploited to violate a system or the information it contains	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

These four key concepts are revisited throughout this report. Various ICT standardization bodies have produced definitions that help to explain the interrelationship between the concepts. The ITU-T Recommendation X.800 and the IETF RFC 2828 defines the above concepts as in Table 1 (ITU-T 1991; Shirey 2000).

The relationship between the threat-related system concepts defined can be illustrated using a simple sketch as shown in Figure 2. Simply put, a successful attack is one that eludes or breaches security countermeasures, consequently taking advantage of system vulnerability and resulting in particular threat consequences or disruptions. Therefore, the success of an attack depends on the strength of the attack, degree of vulnerability and effectiveness of the countermeasures employed.

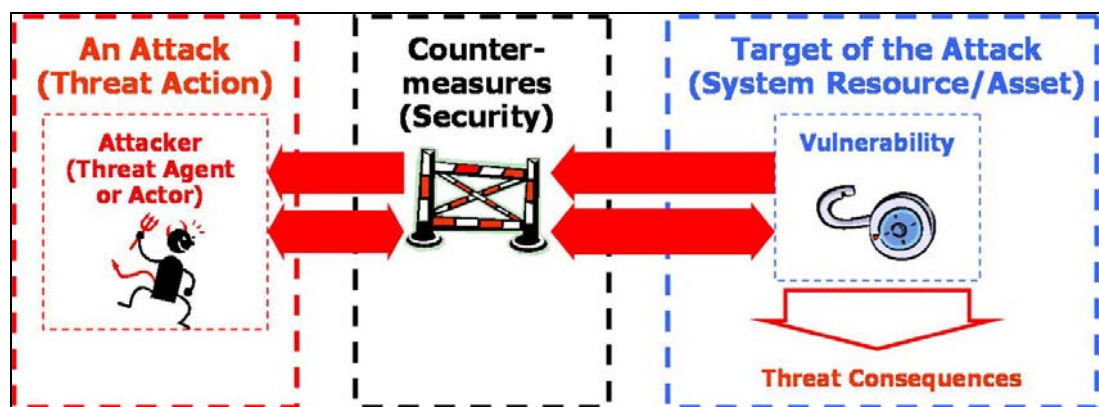


Figure III—2 Relationship between various threat-related concepts.

It is generally acknowledged that it is impossible to secure fully against all attacks (Audestad 2005). This is because ICT systems are growing increasingly complex, making the comprehensive analysis of all failure scenarios computationally intractable. Existing security countermeasures (e.g. firewalls) are implemented against known or predictable attacks and events. However, these measures are not sufficient to protect against the infinitely large number of new, unpredictable and/or unknown attacks that could have a similarly crippling effect on the system. Moreover, the level of implementation of countermeasures and ability to reduce vulnerabilities is constrained by the availability of requisite resources (e.g., sufficient budgets, skilled staff).

Therefore, each organization tries to find a compromise between the level of risk and justifiable information security investment. This necessitates a trade-off between security precautions taken and the tolerance to the remaining risk of attack. Vulnerabilities may be tolerable when the level of difficulty of the attacks needed to exploit the vulnerability is too high, or when the perceived benefit to attacker is small even if the vulnerability is easily exploitable. Conversely, top priority is given to the threat scenarios where the likelihood of attacks is high and their outcomes extremely disruptive. These assumptions are particularly valid for cases when the attacks are well understood and relatively easy to execute, or when the vulnerable system is known to support large user numbers or mission critical processes. All these are typical features that present the prerequisite incentives for potential attackers.

Analysis of the underlying concepts

The analysis of typology and potential scenarios for CII threats (and related concepts) provides the foundation for a comprehensive study of CIIP. This analysis is performed here with the aid of concept maps that make use of a graphical node-arc representation of relationships among a collection of concepts. In concept maps, the concepts are usually represented as nodes enclosed in boxes and then interrelated concepts are then linked using lines with descriptive labels or phrases written over them. These linking phrases specify the relationship between the related concepts. Concept maps are now increasingly used in a diverse range of sectors to articulate and visualize the complex internalities and externalities of various processes.⁴⁸ Notably, concept maps are now also considered as one of the important tools for communicating technical ideas and concepts in the ICT development process (Siau and Tan 2005).

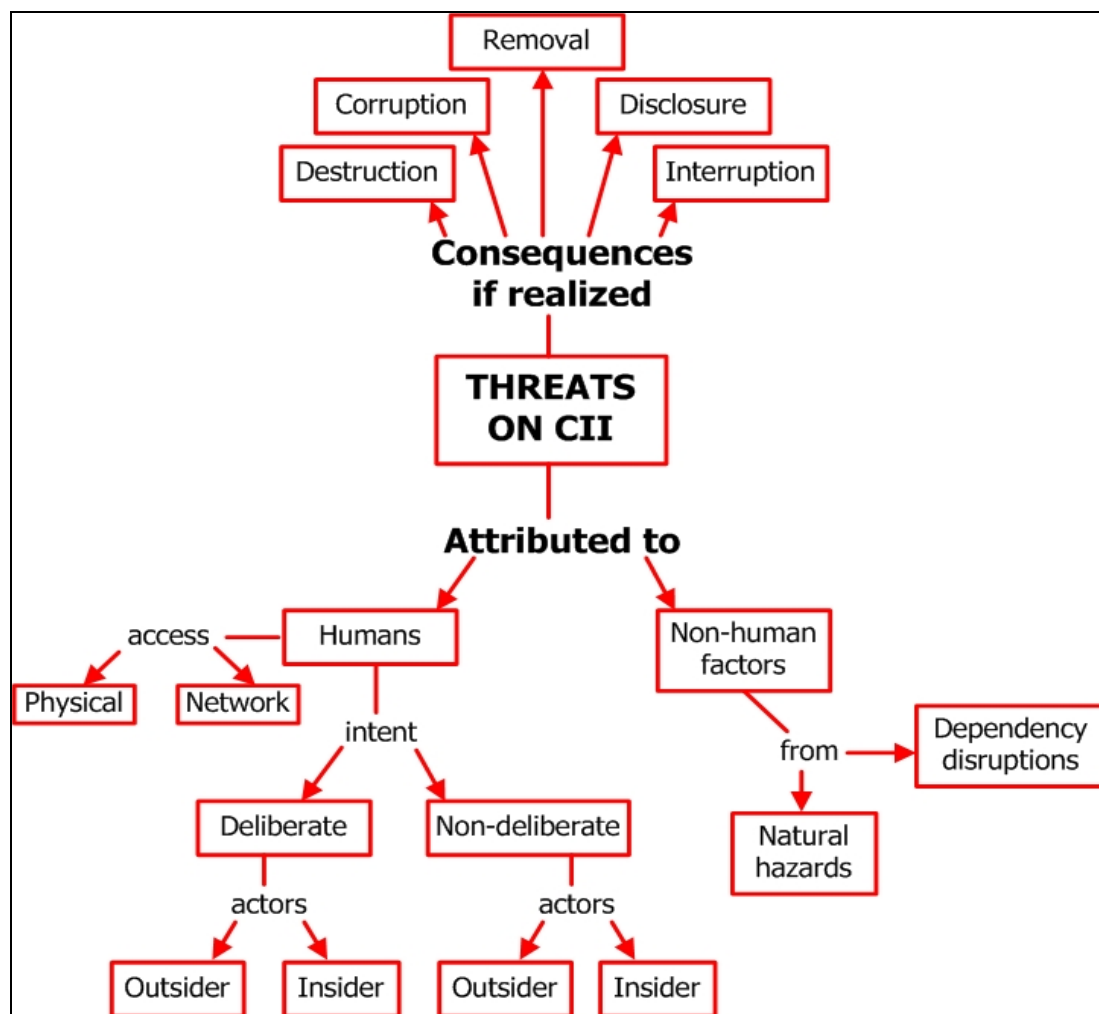


Figure III—3 High-level concept map depicting various aspects of threats on CII.

⁴⁸ For example, a large collection of concept maps produced by the NASA's Center for Mars Exploration (CMEX) detailing various aspects of Mars exploration are available for public viewing (CEMEX 2007).

A concept map originating from the concept of threats on a CII would be rather large and cumbersome to depict with sufficient clarity on a single integrated map. Therefore, a high-level concept map representing only the major concepts (the nominal ‘view from 50,000 feet’) can be seen in Figure 3. The map is derived from an extensive survey of standardization documents (ITU-T X.800 and RFC 2828), technical notes from industry (Gordon 2003; Albert et al 2003), general scientific literature (Stallings 2003, Rozenblit 2000, Vacca 2006, Yoo 2005) and a multitude of online material. It is clear from Figure 3 that threats to CII are attributed to a range of factors that exploit system vulnerabilities and if realized will result in any of a possible set of consequences to the system. Further explanation of these initial observations is provided in the subsequent subsections with the aid of detailed low-level concept maps.

Consequences of Threats

The successful realization of a threat on a CII would result in at least one of the following outcomes:

- The destruction of information, system assets or resources.
- The corruption or modification of information.
- The theft, removal or loss of information, system assets or resources.
- The undesired or unauthorized disclosure of information.
- The interruption of service delivery.

The methods or action leading to each threat consequence may vary, as illustrated in Figure 4. Destruction, removal or interruption could potentially lead to the partial or complete failure of the system to function and provide intended services. This, for example, could be the result of the physical destruction of a main switching centre that weakens the ability to exchange information between geographically distant areas, or a prolonged denial-of-service (DoS) attack that illegally consumes limited system resources and makes an asset (e.g., website, server etc.) unavailable. Distributed DoS (DDoS) attacks are even more intense, as they use multiple compromised systems or zombies to launch simultaneous attacks on a target system.

On the contrary, corruption, disclosure or removal of information may not directly lead to system failure, but may enable unauthorized access to system data that could be used to launch more severe attacks on the system, comprise operations of organizations relying on the system (e.g. leakage of information from a military network revealing troops positioning), or even as part of a more sinister plot. For example, it is believed that the bombers behind the 2004 attack on the Madrid commuter train had planned their attack using fraudulent telephone calls made by hacking in to a telephone exchange (a practice commonly known as ‘phreaking’) belonging to a bank in France (Pollard 2005).

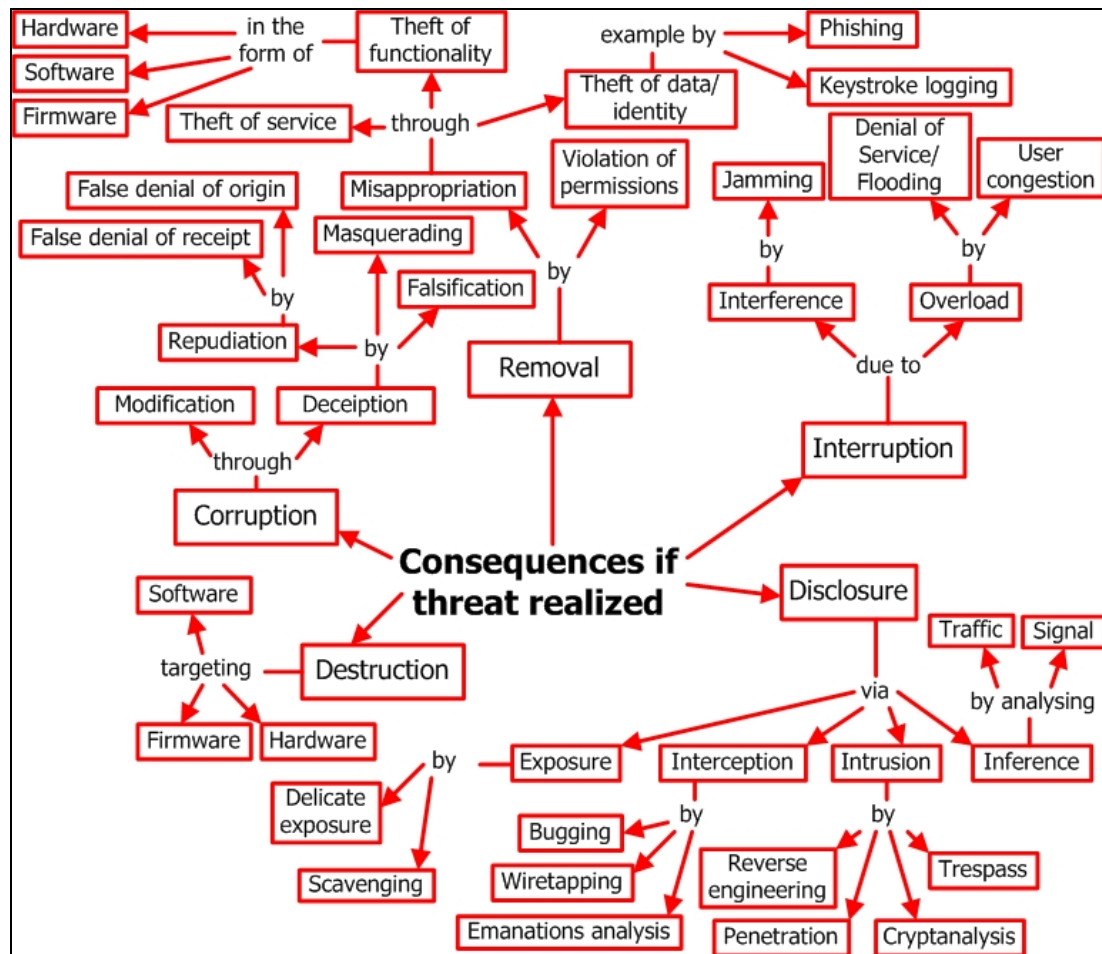


Figure III—4 A low-level concept mapping of the consequences of realized threats.

Nature of the Threats, Part I – Non-Human Factors

Threats to a CII may originate from a wide range of human or non-human factors, as illustrated in the concept map of Figure 5.

Non-human factors are those whose resulting threats cannot be directly attributed to human actions. This includes the events briefly outlined below.

I. Natural hazards

Natural hazards have the potential to cause direct physical destruction to CII and CI in deployed the areas affected by the hazard, leading to widespread disruptions (common- cause failures). For CII, elements such as aboveground transmission lines, poles, towers and telehousing facilities, could be damaged by winter storms, forest fires, earthquakes and so forth. Moreover, heavy downpours and flooding could disrupt access holes and damage underground telecommunication cable plant. The average hazard intensity class of past occurrences of various natural hazards in the BSR is shown in Table 2.⁴⁹ Additional investment would usually be required to reinforce CII against high-intensity hazards. This requirement is further

⁴⁹ The average BSR hazard intensity is loosely derived from hazard intensity maps produced in the EU ESPON 2006 project 1.3.1 (Geological Survey of Finland 2006).

exacerbated by the fact that current trends in climate change (e.g. rising sea levels resulting in severe floods) would lead to future intensity increases for some hazards. For example, climate-change induced sea level rises will be a major cause of flooding in parts of the BSR in the coming decades (Schmidt-Thome 2006).

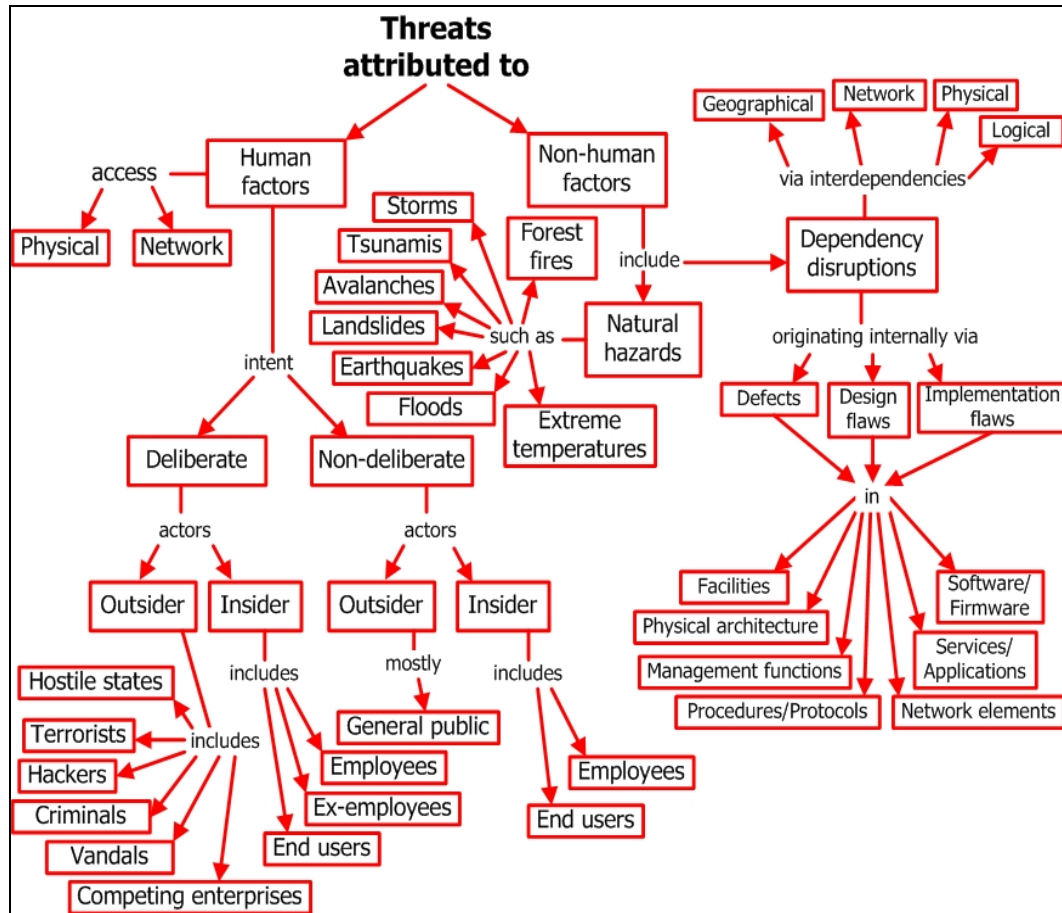


Figure III—5 A low-level concept mapping of the possible nature of threats.

Table III—2 Average intensity classification of past occurrences of natural hazards in the BSR.

Average Hazard Intensity Classification	Hazard Types
Class 1: Very low	Earthquakes; Floods; Tsunamis and Volcanic eruptions.
Class 2: Low	Forest fires
Class 3: Medium	Extreme temperatures and Landslides.
Class 4: High	Storms (mostly winter storms)
Class 5: Very high	Avalanches (mostly in Norway and parts of Sweden)

II. Dependency Disruptions

Critical information infrastructure is typically engineered with integrated fault recovery mechanisms to guarantee a five-nines (99.999%) availability, which translates to less than 5.25 minutes of total unplanned system downtime per year (Kimber et al 2006).⁵⁰ Internal failures usually result from defects or flaws in hardware, software, procedures, management functions and so forth. The complex mutual dependency and interconnectivity between different critical (information) infrastructure means that the effects of failures or their ensuing disruptions may cross infrastructure boundaries. This crossover is manifested in the triggering or cascading of new failures, or even aggravation (escalation) of existing failures in interdependent infrastructure (Rinaldi et al 2001). A CII would typically have multiple interdependencies with other infrastructure. These include physical interdependency due to need for resources from another infrastructure;⁵¹ geographical interdependency due to collocation or close proximity with other infrastructure; and networked or cyber interdependency whereby the commodity exchanges between dependent infrastructures is information.⁵² Moreover, logical interdependency accounts for those complex relationships that are not easily associated with any of the aforementioned interdependency categories.

Nature of the Threats, Part II – Human Factors

Threats attributed to human factors are carried out by threat actors whose threat actions either have a deliberate or non-deliberate (accidental) intent. The positioning of the threat actor also varies. They may be within a designated security perimeter (insiders) or outside the parameter (outsiders). Insiders include end-users or customers with basic access to services delivered over the CII, and employees of the organization operating the CII. Access for insiders is enabled by the use of passwords, PIN codes, smartcards, biometric identification, building keys, and so forth. Employees would naturally have more privileged access to system resources and assets, in comparison to end users. This enables employees to carry out their various responsibilities within CII organization. These employees range from key personnel responsible for system Operations, Administration, Management and Provisioning (OAM&P) of the CII to housekeeping staff that maintain the cleanliness of the facilities. The type and degree of access privileges accorded to employees also varies depending on their job description within the organization. For instance, access privileges may be restricted to just a subset of

⁵⁰ In practice, planned system downtime (e.g., for equipment upgrades, routine maintenance, software patches, re-calibrations, system reboots etc.) tends to be more frequent, and is usually accounted for outside the 5.25 minutes downtime per year requirement. Planned downtime inconvenience is eased by scheduling by giving advance notice on maintenance windows to prepare users for service disruptions.

⁵¹ The most common physical dependency is need for a clean constant supply of electrical power to operate CII facilities such as network switches, servers, transmitters and so forth. However, electricity obtained from the public utility is often unavailable (blackouts) or corrupted (e.g., by power surges, sags, transients etc.) that switch off or damage CII equipment. Preventive measures include the use of localized backup power, proper grounding, surge protection and power conditioning.

⁵² An example is when one information infrastructure (e.g. national backbone network) is used to aggregate or backhaul information traffic from other information infrastructures.

operations or to only a few hours during some days of the week. A typical illustration of access accorded to different groups is depicted in Figure 6.

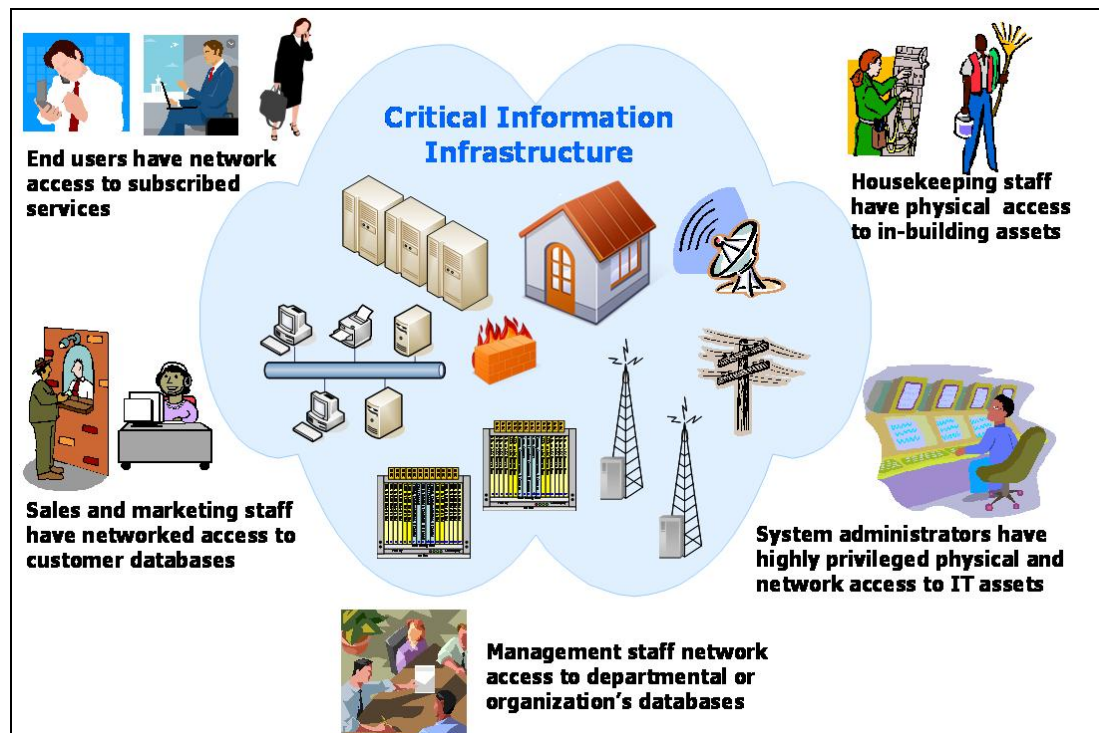


Figure III—6 Example of type of authorized access accorded to different groups.

I. Deliberate Threat Actors

The threat actors with deliberate intent have in great part put into focus the need for CIIP. These actors are profiled briefly in Table 3. The threat posed by hackers has long been recognized within the IT security community, with anti-hacking security measures being the norm and legal procedures regularly instituted against those responsible. Continued increases in electronic/mobile-commerce activities⁵³ create added incentive for criminal activity (cyber-crime)⁵⁴ and fuelling unfair practices between rival companies via the information infrastructure.⁵⁵ Hostile governments are also recognizing the increased potential of undermining adversaries by launching attacks that disable their CII (Overill 2001).

Of the threat actors mentioned in Table 3, the threat posed by terrorists is currently the most widely publicized. Thus far, terrorist attacks have targeted more visible or tangible critical infrastructure, such as railways, airports, water

⁵³ For example: eMarketer (eMarketer 2007) predicts electronic commerce retail sales in Europe will reach USD 400 billion by 2011; Finextra (Finextra 2007) predicts global mobile commerce market (excluding mobile entertainment) to grow to USD 40 billion by 2009.

⁵⁴ Cyber-crime refers to traditional crime activities facilitated by the use of ICTs. The proliferation of cyber-crime has prompted the Council of Europe to draw up a "Convention on Cybercrime (CETS No.: 185)," a first international treaty (with 43 signatories) on crimes committed via the Internet and other computer networks.

⁵⁵ For example, a Massachusetts businessman is known to have authorized crippling DDoS attacks against three competing companies (Poulsen 2004).

distribution systems and so forth. To that end, terrorists have eschewed traditional hierarchical, top-down command structures, opting to operate in covert cells that are increasingly internationalized and decentralized, so as to limit damage to the operations of the main terrorist organization when a cell is captured. Terrorists actually rely on the efficiency, pervasiveness and relative anonymity afforded by the Internet (in comparison to the physical world) to coordinate terror operations between cells, build new alliances, raise funds globally, make press releases and market their ideology.

Table III—3 Brief overview of actions and positioning of various deliberate CII threat actors.

Threat Actors	Positioning	Motives of Deliberate Threat Actions	Intended Consequences of Threat Action
Terrorists (cyber-terrorism)	Outsiders	Spread fear/panic, disrupt normal operations, ideological statement, seek publicity, inflict mass casualties	Interruption, destruction
Hackers/crackers/phreakers	Outsiders	Monetary gain, intellectual challenge, power/pride, status/peer recognition, hacktivism (environmentalism, anti-globalization etc.), nationalism, extremism, self-expression, youthful frivolity, mischief, thrills, experimental curiosity	Interruption, destruction, corruption, removal, disclosure
Hostile states	Outsiders	State-sponsored espionage, gain military or strategic advantage, censorship, spread propaganda	Interruption, destruction, corruption, removal, disclosure
Rival companies	Outsiders	Industrial espionage, gain economic and competitive advantage	Removal, disclosure
Criminal/crime organizations (cyber-crime)	Outsiders	Monetary gain, extortion/blackmail, intimidation, peddling illegal content (e.g., child pornography)	Interruption, destruction, removal, disclosure
Vandals/defacers	Outsiders	Disrupt normal operations, seek publicity, mischief	Destruction, corruption
Employees/ex-employees/contractors/temporary workers	Insiders	Personal grievances, vengeance, monetary gain, espionage, experimental curiosity	Interruption, destruction, corruption, removal, disclosure
End-users/customers/subscribers	Insiders	Personal gain	Removal, disclosure

As Der Derian described it so vividly:

“Over the last few weeks the world has received a crash course in network warfare. Al Qaeda members reportedly used encrypted email to communicate; steganography to hide encoded messages in web images (including pornography); Kinko's and public library computers to send messages; underground banking networks called hawala to transfer untraceable funds; 24/7 cable networks like Al-Jazeera and CNN to get the word out; and, in their preparations for 9-11, a host of other

information technologies like rented cell phones, online travel agencies, and flight simulators. In general, networks -- from television primetime to internet realtime -- delivered events with an alacrity and celerity that left not only viewers but decision-makers racing to keep up.” (Der Derian 2001)

However, whilst relying heavily on ICTs for their operations, terrorists also recognise the potential of possible widespread cross-sector disruptions that could be caused by an attack on CII and are known to be actively pursuing various attack options. For instance, an ‘Electronic Jihad Program’ for launching DDoS attacks on websites selected by the attacker was reportedly available for download from the jihadi website Al-jinan.org (Greenemeier 2007). Interestingly, a very thin line now separates terrorist and criminal tactics, as crime organizations are now adapting the loose structure of terror organizations, whilst terror organizations employ criminal actions to fund their activities. For instance, the illegal drug trade provides a vital source of income for terror organizations, a phenomenon labelled ‘narco-terrorism.’ (Erhenfeld 2002) Therefore, as the gains from cyber-crime continue to rise,⁵⁶ terrorists will almost certainly look to supplement their income by engaging in cyber-criminal activities (Shelley 2003).⁵⁷

Vandalism against CII may take various forms. By far the most prevalent act of vandalism is the defacement of websites; a form of digital graffiti, whereby, a vandal or defacer replaces the contents of a hosted website with their own.⁵⁸ Whilst the motivation by the defacer may only be mischievous, the fact that websites are key storefronts in the age of e-commerce implies that a defaced website may result in lost revenue due to the reluctance of customers to conduct transactions via the website. Furthermore, website defacement is now becoming a very visible form of protest or of making a statement, such that the technique is now being used by more extreme threat actors such as terrorists, nationalists, extortionists and so forth.

Insiders also represent a significant threat by virtue of the access they have within a CII (see Table 3). Research by Gartner indicates that up to 70% of security breaches originate internally from employees (Mogul 2002). End users could also become threat actors by abusing their limited access to a system, for instance, by trying to access services outside their subscription agreement or sharing their access right with unauthorized users.

II. Non-Deliberate Threat Actors

Insiders’ may become unwitting threat actors due to non-deliberate or subconscious actions, such as negligence, ignorance or even inadvertently exhausting a system’s resources (see Table 4). A common scenario is that of public mobile communications networks getting jammed (overloaded) during unplanned

⁵⁶ For instance, a statistic offered by the online security company Garlik (2007) indicates that in Britain “there is a new victim of cyber-crime in every ten seconds,” See also: Thomas & Martin (2006).

⁵⁷ Shelley (2003) notes that the ease and security, with which transnational criminals and potential terrorists can transmit information, will provide a challenge in many areas that are not even foreseen at the present time.

⁵⁸ An example archive of defaced websites is published by (Zone-h 2007).

mass gatherings, or in the aftermath of a sudden catastrophe, whereby an uncharacteristically large number of subscribers attempts to call or text friends and family at the same time. Members of the general public may also disrupt system operations by accidental damage to a system asset. Accidental telecommunication cable cuts due to construction or farming activities are a common cause of large-scale service outages. For example, an accidental double cable cut in Sprint's backbone network in January 2006 left millions of their fixed and wireless customers cut-off for over three hours in the west coast of the USA (Poulsen 2006).

Table III—4 Brief overview of actions and positioning of various non-deliberate CII threat actors.

Threat Actors	Positioning	Cause of Non-Deliberate Threat Actions	Unintended Consequences of Threat Action
General public	Outsiders	Accidental damage to system assets	Interruption, destruction
Employees/contractors	Insiders	Negligence, sloppiness, human error, omission, fatigue, insufficient or poor training, incapacitation	Interruption, destruction, corruption, removal, disclosure
End-users/customers/subscribers	Insiders	Carelessness; inadvertent system overload	Interruption

Methods of Attack

The previous subsection highlighted potential threat actors and their possible motivations for carrying out attacks on a CII. Although their motivations may differ significantly, the attack methodologies employed by different actors may be the same. For instance, a cyber-criminal, hacktivist, terrorist and website defacer may exploit the same vulnerability to break into a web server even if it is for totally different reasons. Threat actions on a CII can be executed by the threat actor gaining physical access to the CII or remotely using network-based connections provided by the CII itself. The former has been the access method of choice for deliberate threat actors intent on disrupting or inflicting physical damage on infrastructure. For example, a threat actor may deliver chemical agents or explosive devices (e.g., person-borne, by vehicle, by post etc.) to a physical site of a critical infrastructure with an intention of incapacitating key personnel (e.g., system administrators, train driver, security guards etc.) or damaging critical assets (e.g., server farms, telephone exchanges, train carriages, power transformers etc.).

Information infrastructure also presents a unique security challenge, whereby network-based access enables delivery and execution of threat actions, with the end results being just as debilitating to the system as a physical attack. The targets of these attacks are non-tangible information flows, stored data, network resources or software resident in the system. The threat is delivered in the form of *malicious logic*, a blanket term defined in IETF RFC 8282 to refer to any hardware, software, or firmware that is intentionally included or inserted in a system for a

harmful or undesired purpose (Shirey 2000). This is further illustrated in the concept of map Figure 7.

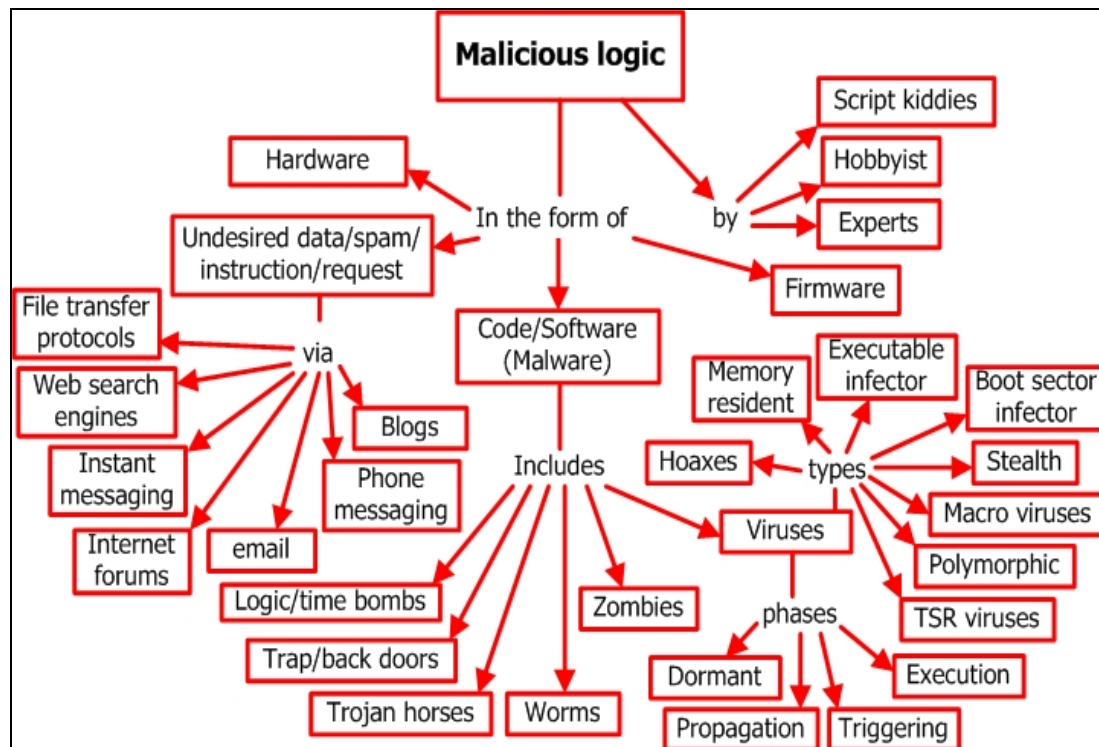


Figure III—7 Concept mapping of malicious logic in information and communication systems.

Malicious software or malware has long presented a significant security threat that has become more pronounced with the ubiquitous connectivity enabled by the Internet.⁵⁹ As an indication of existing threats, in a recent ‘honey pot’ experiment a computer running Windows XP (Service Pack 1) with no anti-software software was connected to the Internet and ended being successfully infected by worms within 18 minutes, and in one week was scanned over 46,000 times by remote computers looking for vulnerabilities (Wehner 2006). Attacks on CII using malicious logic is quickly becoming the preferred modus operandi for various deliberate threat actors, since such an attack has a very low cost of entry, is effective in the disruption it causes, and carries a low risk of being apprehended. The proliferation of undesired data (spam) in information and communication systems also constitutes a threat, in the way that the delivery, filtering and subsequent deletion of this unsolicited data consumes valuable bandwidth, storage and human resources. Some security analysts now believe that the volume of e-mail spam is increasing at levels that are threatening the viability of global e-mailing system (Gillis 2007)⁶⁰.

⁵⁹ For example, the infamous ILOVEYOU worm managed to infect 10% of all computers connected to the Internet in just one day of May 2000, leading to damages in the range of €4 to €7 billion.

⁶⁰ A study by Gillis (2007) estimates that e-mail spam volume doubled in the period between October 2005 - October 2006, vastly outnumbering legitimate e-mail messages. Critically a third

Threats on the Underlying Information Infrastructure for CI

The system monitoring, control and status data gathering in most CI are now automated processes with reduced reliance on human effort. These processes rely on SCADA (Supervisory Control and Data Acquisition) networks that enable communication with remote units using industrial protocols, such as, Modbus and PROFIBUS (Process Field Bus). Traditionally, SCADA networks have been considered to be closed networks and so security was not addressed in great depth compared to conventional ICT systems.

However, recent trends have seen open standards and Internet technologies being increasingly adapted in SCADA networks. This is partly driven by the need to share up-to-date status data (e.g., with supply chain partners) and minimize expenditures by, for instance, reusing corporate network infrastructure and leased lines to implement parts of the SCADA network. Unfortunately, these measures provide direct or indirect connectivity points to the Internet and other public networks, creating a security gap that can end up compromising the systems controlled by the SCADA networks (Graham and Maynor 2006). Many examples exist of previous security breaches in SCADA networks. For instance, in March 2000, a disgruntled ex-employee in Australia repeatedly hacked into a sewerage management system releasing over a million litres of raw sewage into public places. And in January 2003, the Slammer worm disrupted SCADA traffic causing operators to temporarily lose some degree of control of the Davis-Besse nuclear power plant in Ohio USA. As a result, there is now increased acknowledgement of the possibility external attacks on SCADA networks by CI owners, and a notable surge in interest in SCADA systems by terrorists groups (Naedele 2007).

Recent information security trends in the BSR

Most of the nations of the Baltic Sea Region (BSR) epitomize what are known as information societies, and their achievements in this regard are routinely used as yardstick by other countries. This assertion is justified by the global rankings of various ICT indices (e.g., Knowledge Economy Index⁶¹, Networked Readiness Index⁶², ICT diffusion Index⁶³ etc.), where the BSR countries feature prominently in top tier of the rankings. Paradoxically, highly advanced information societies are usually left exposed to new kinds of vulnerabilities, as attested by the select examples below describing in brief some realized information security threats in the BSR.

- *Example 1:* Users of Nordea's personal Internet banking service in several countries in the BSR are regularly targeted by fraudulent phishing

of that spam is now image-rich e-mail spam message (about three times the size of a text only e-mail spam), thus speeding up the exhaust of bandwidth and e-mail gateway capacities.

⁶¹ World Bank's Knowledge Economy Index (KEI) evaluated based on variables representing conduciveness of economic and institutional regimes; educated and skilled population; efficiency of innovation environment; and use of ICTs.

⁶² World Economic Forum's Networked Readiness Index (NRI) measures a country's preparedness to exploit the opportunities offered by ICTs.

⁶³ United Nations Conference on Trade and Development's ICT diffusion index (ICTDI) measures a country's penetration of ICTs (that is, mobile/fixed phones, Internet hosts and PCs) and its affordability.

attacks, luring them to disclose their bank codes. Earlier attacks in October 2005 forced the temporary closure of the service in Sweden and later actually succeeded, causing a reported loss of over €900,000 from user accounts as of January 2007 (Libbenga 2007). Most of the bank's websites now post detailed customer advisory notes on how to deal with phishing attacks⁶⁴.

- *Example 2:* A malfunctioning of a 220 kV power transmission line in Uppsala 2nd October 2002 caused outage in fixed and mobile communication networks in northern parts of Stockholm, Uppsala, Västerås, and so on. Consequently, the network failures triggered cascading failures affecting terrestrial television and radio broadcasts in some areas, the radar at Stockholm-Arlanda airport causing flight disruptions, and also rail system causing trains to run late (Eckström 2004).
- *Example 3:* The Estonian government moved a Soviet war memorial statue from a central square in Tallin on 26th April 2007. For the next three weeks, websites belonging to Estonian government departments (e.g., all ministries, except those of Culture and Agriculture) and businesses come under unusually intense but coordinated DDoS attacks. The Estonian authorities were then obliged to block overseas Internet connections to enable locals to continue accessing essential online services provided by key Estonian websites (Lesk 2007; Rantanen 2007).
- *Example 4:* In August 2007, hackers infiltrated a database belonging to the telecom operator Tele2 and managed to steal details of 11-digit personal identification (ID) numbers and home addresses belonging to over 60,000 Norwegians. Among the victims is the head of the national data inspectorate, Datatilsynet. The stolen details put the victims under the serious threat of identity theft. The Norwegian police subsequently urged increased vigilance by the victims and are investigating the matter (Solberg 2007).

A more general snapshot of a country's overall information security trends is typically provided by national CERTs (Computer Emergency Response Teams) or CSIRTs (Computer Security and Incident response Teams). CERTs/CSIRTs offer a one-stop-shop service for reporting all security incidents (e.g. break-ins, DDoS attacks, new malware, discovered vulnerabilities etc.), publishing threat alerts and provisioning advisory services for a nation's information security communities. Therefore, the statistics of security incidents compiled by a national CERT/CSIRT are usually quoted when analyzing information security trends for a particular country. For instance, the statistics obtained from the Finnish CERT (CERT-FI) indicate a sharp rise in reported security incidents since 2002 (see Figure 8). Notably, the number of reported incidents in the first half of 2007 already exceeds

⁶⁴ See for example Nordea Finland (2007).

incidents reported for the whole of 2006. Similar information security trends are mirrored elsewhere in the BSR⁶⁵.

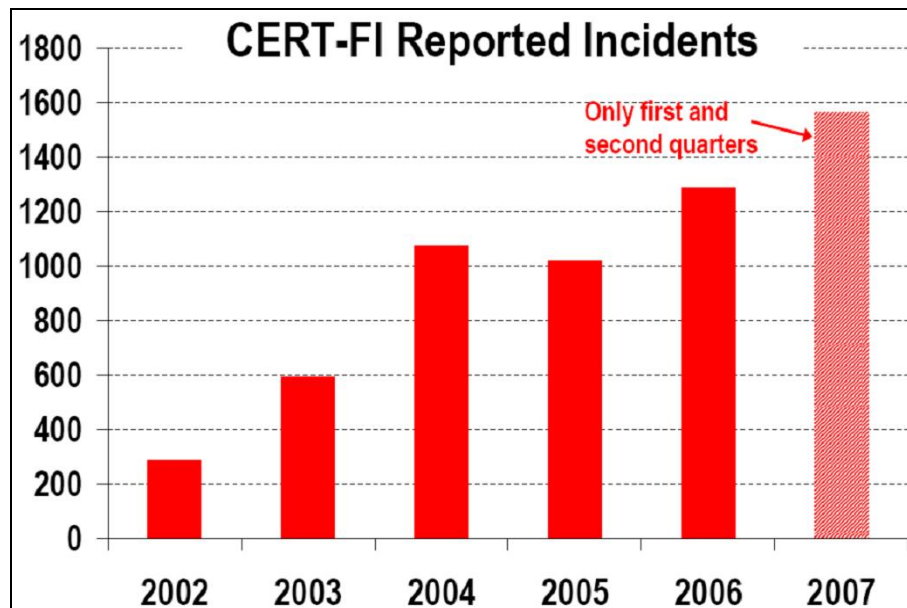


Figure III—8 CERT-FI reported incidents between in the period between 2002 and 2007.

Regardless of the examples and trends described above, it would be an exaggeration to describe the information security situation in the BSR as dire. The security breaches have mostly caused inconveniences, minor displeasure, some anxiety and limited monetary losses. However, the future signs are ominous and there is possibly a slight shift in public opinion, as noted in a recent editorial in one of Finland's high circulation newspapers (Turun Sanomat 2007):

“The rise in Internet crime and vandalism will surely slow down the enthusiasm to move services to the net and use them. In this sense the Internet attacks and fraud represent a setback to those who believe in the information society. From the perspective of crisis preparedness, it seems more and more sensible, in the light of recent events, to maintain the old systems for information transfer and storage. An old trick may not be better than a bag of new ones, but the old way of doing things may sometimes be indispensable”

Such sentiments go a long way in emphasizing the practical need for CIIP in the BSR, which happens to be the main theme of this report.

⁶⁵ An inventory profiles, links to reports and contact information for CERTs/CSIRTs of each of the countries in the BSR and the rest of Europe is maintained by the European Network and Information Security Agency (ENISA 2007).

3.2 CASE STUDY ON CIIP

This section focuses on the selected case study on CIIP. The first and second subsections describe the CII selected for the study. The third subsection provides an extended description on a selected security assessment methodology that is then used to assess the security and protection of study CII in the fourth subsection.

Professional mobile radio as a case study

The ICT landscape is now a complex ecosystem of systems based on any one of several possible technology standards using equipment from multiple vendors. Moreover, each of these systems is operated by different entities but with complex inter-operator agreements and targets a diverse range of end users, each with their own special requirements. Figure 9 provides a snapshot of the communication systems whose services are likely to be accessible to end-users in any given area of an industrialized country. This report focuses on professional mobile radio (PMR)⁶⁶ networks as a CII for the CIIP case study.

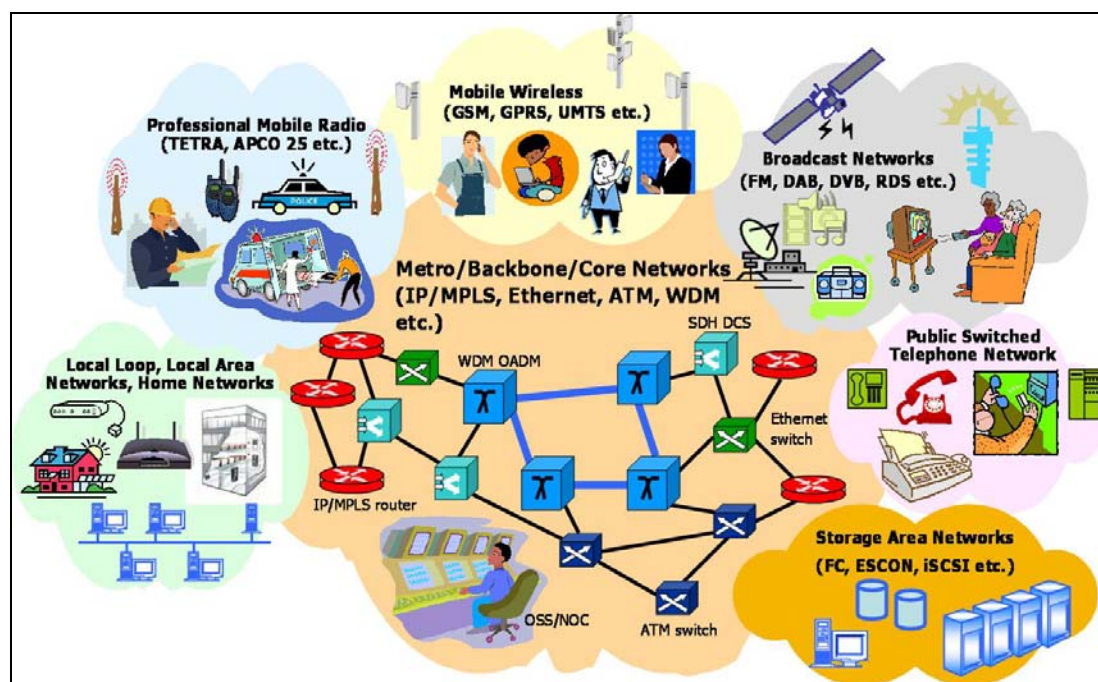


Figure III—9 Illustration of the diverse ICT landscape.

PMR networks are not just crucial in their own right; they are also crucial in ensuring the safety and security of people and other critical infrastructure. The end users of PMR tend to be professionals who depend heavily on communication tools for their work and cannot afford that PMR services are unavailable, particularly in moments that demand a decisive response (Ketterling 2004). This includes those working in emergency services, public safety and security agencies, local government administration, disaster relief, environmental protection,

⁶⁶ Alternatively referred to as Private Mobile Radio in some literature.

utilities, industrial operations, construction sites and the management of major public events. The critical nature of the tasks carried out by these professional users means that they cannot rely solely on less robust public (mostly commercial) communication networks for their work. The service provided by public networks is more likely to be corrupted by security breaches or be totally unavailable during critical situations. By contrast, PMR networks and MSs are specifically designed to guarantee security and high service availability at all times. Moreover, low PMR terminal and infrastructure costs provide optimum cost to coverage ratio, this being an essential cost parameter since the PMR user base is generally smaller compared to public networks.

The case of the 7/7 London bombings⁶⁷ is a useful example in illustrating the aforementioned points. In the immediate aftermath of the bombing, public network operators reported very sharp increase in the number of call attempts. The surprise nature of the attack meant that the operators had no time to re-engineer their networks to handle this extra traffic, and hence most of the calls ended up being blocked (that is, callers got excessive busy tones). This lack of reliable communications seriously hampered the emergency response and rescue effort. A report by the 7 July Review Committee noted, among others, the following failings (Greater London Authority 2006):

- Congestion in public networks left some senior emergency staff (who were relying on public mobile communications) isolated from other field teams and control room staff.
- Lack of communication facilities between the passengers and train drivers increased the level of panic for passengers in the targeted trains.
- Lack of reliable communications between train drivers and line controllers, as the antennas were damaged in the explosion. It was further noted that the existing system suffered service interruptions in blind spots within the tunnels.
- Inadequate or non-existent communications from trains to emergency services and the London Underground Network Control Centre. This meant that after the bombings emergency workers had to run from trains to platforms to be able to communicate with colleagues and supervisors above ground.

In the light of these failings, the 7 July Review Committee recommended that digital PMR networks are fully implemented for all of London's emergency services and within its underground transport network (Greater London Authority 2006).

Overview of TETRA: A digital PMR standard

Development of the TETRA Standard

The use of analog PMR technology is recorded as early as the 1920s in the USA and the 1950s in Europe⁵⁴. In the subsequent decades different analog PMR

⁶⁷ The bombings on 7th July 2005 were carried in four separate locations in London's transport system, killing 52 people and injuring over 700 people.

solutions were developed in Europe with varying properties (e.g. frequency, bands, channel separation, transmit power etc.). This disparity made interoperability difficult and limited production volumes of each PMR type, hence driving up costs. These problems, coupled with the performance limitation of analog systems, created the need for a standardized digital PMR system. To that end, the European Telecommunications Standardization Institute (ETSI) eventually produced an open and harmonized digital PMR standard (EN300-392 series) known as TERrestrial Trunked Radio (TETRA). Furthermore, a TETRA MoU Association representing users, equipment manufacturers, application providers, integrators, operators etc., was created in December 1994 to promote TETRA globally. The TETRA standard incorporates features of mobile telephony, mobile data and mobile radio systems, and is widely viewed as a replacement for the fragmented analog PMR systems that have been used previously by different authorities.

Alternative digital PMR standards have been produced in other regions, most notably the APCO-25 standard used in North America.⁶⁸ Several proprietary digital PMR systems such as iDEN (by *Motorola*), EDACS (by *General Electric/Ericsson*) and TETRAPOL (by *EADS Telecom*), are also in use, although their market share is not as large as the open standard systems. The latest trends for the implementation of nationwide public safety and security (PSS) networks in the BSR is seen to widely favour the TETRA standard, as indicated in Table 5.

Table III—5 Existing status of PSS TETRA network implementations in the BSR as of early 2007. (TETRA MoU Association)

Country	Status of nationwide PSS TETRA network implementations as of early 2007
Denmark	Nationwide network in planning/procurement phase.
Estonia	Existing sharing agreement with the Finnish network (VIRVE) along the Gulf of Finland and northern coast. Nationwide network (EDTN) being implemented, to be completed by 2008.
Finland	Nationwide network (VIRVE) completed in 2001 and operational since 2002.
Germany	Nationwide network (BOSNet) being implemented, to be completed by end of 2010.
Latvia	Non-TETRA nationwide network operational.
Lithuania	Nationwide network being implemented, scheduled for completion in late 2007.
Norway	Nationwide network (Nodnett Project) being implemented from mid 2007.
Poland	Sub-national network operational. Nationwide network in planning/procurement phase.
Sweden	Nationwide network (RAKEL) being implemented, to be completed nationwide by 2010.

TETRA Mobile Stations and System Architecture

The mobile stations (MSs) or user terminals⁶⁹ for TETRA systems are typically rugged handheld terminals⁷⁰ that visually resemble conventional mobile handsets

⁶⁸ APCO-25 standards were produced by the Telecommunications Industry Association (TIA). Complications in IPR (intellectual property rights) licensing has meant that APCO-25 is the leading digital PMR standard in the US rather than TETRA, despite of the fact that the latter has more functionalities and lower cost per subscriber. See also Bishop (2001).

⁶⁹ In this chapter, the terms “MS” and “terminal” will be used interchangeably.

(see Figure 10), but differ in various essential functionalities provided. Furthermore, slightly larger vehicle-mounted terminals with higher output power⁷¹ are also available for high mobility users whose individual responsibilities cover a large area, such as police in squad cars or on motorcycles. Moreover, a stripped-down version of MSs may be used for machine-to-machine communications in wireless telemetry (that is, remote measurements and monitoring over a wireless network) applications.



Figure III—10 Handheld and vehicle-mounted TETRA mobile stations. (EADS Secure Networks)

TETRA networks are cellular mobile communication systems, so a geographical service area covered by a TETRA network is usually divided into multiple smaller areas or cells. This cellular arrangement enables the limited radio frequency resources to be efficiently reused in non-adjacent cells. TETRA users located in a particular cell are then able to communicate over the TETRA network via a base station (BS) that provides radio coverage within that cell (see Figure 11).

A BS constitutes antennas atop a radio tower or tall building and a small facility housing the equipment for radio transmission/reception. When mobile users on a call travel between one cell and another, their conversation is handed over between the cells to enable uninterrupted communications. A typical city or region would have hundreds of BSs and these are connected to a Mobile Switching Center (MSC) that controls the multiple BSs, provide switching functions, coordinate location updating and manage user mobility between different cells. The network-wide operations are overseen by a network operations center handling functions such as network management, billing, customer care and so forth. All the MSCs, BSs and the network management system (NMS) in a TETRA network are collectively referred to as the Switching and Management Infrastructure (SwMI).

⁷⁰ Mostly to be found in belt-worn or shoulder-mounted positions.

⁷¹ Vehicle-mounted terminal have an output power around 5-10W, compared to 1W for handheld terminals, enabling the former to have relatively better coverage.

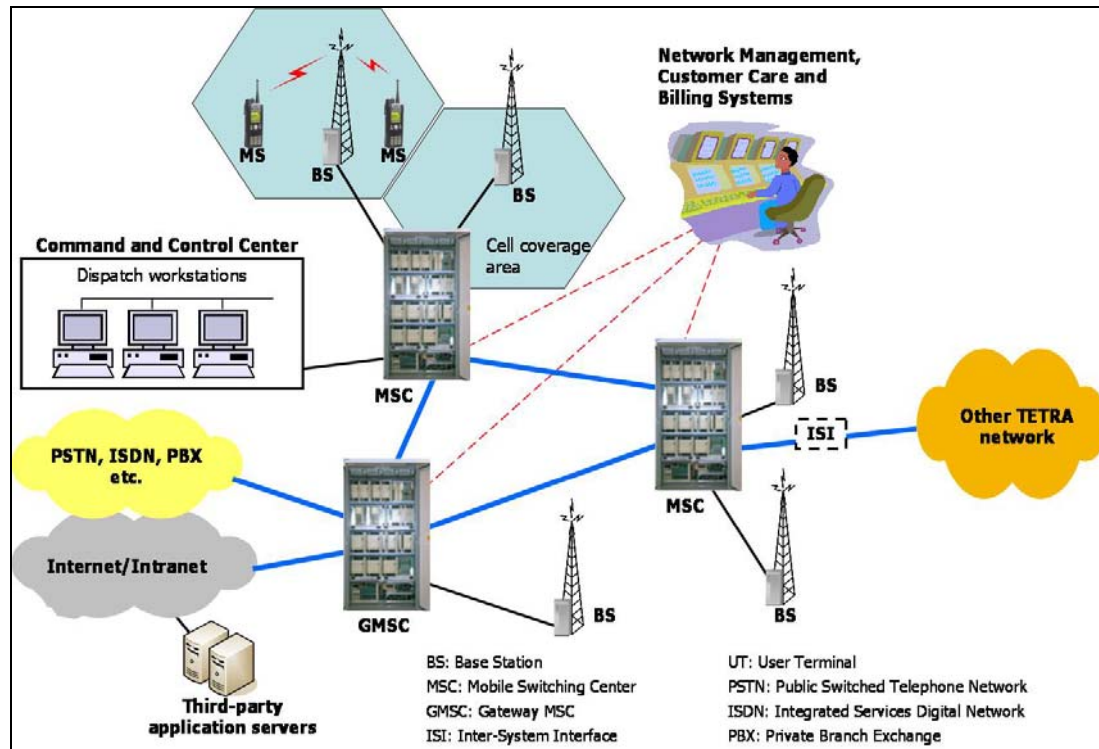


Figure III—11 Example architecture of a TETRA network.

The connectivity to TETRA networks operated and administered by other organizations is provided over an Inter-System Interface (ISI) between SwMI of the two networks. Furthermore, connectivity to non-TETRA networks (e.g. the public switched telephone network) is provided via a Gateway MSC (GMSC). The interconnection of multiple MSCs enables implementation of TETRA networks with regional or nationwide coverage. Furthermore, APIs (Application Programming Interfaces) can be provided to enable the smooth integration of network applications developed by third parties. Unique to PMR systems is the presence of a command and control centre with dispatchers whose primary function is to control and coordinate communication of users or members of a user group belonging to a particular agency or authority. Dispatchers are able to fulfil those roles by having a broad view of the situation in an unfolding event. For instance, a police force dispatcher upon confirmation of the location of a reported crime scene on their workstations may identify and instruct the police squad car in the closest vicinity to proceed to reported crime scene.

Brief Technical Description

TETRA has basic architectural similarities with public mobile communication systems such as GSM (Global System for Mobile communications).⁷² The main distinctions are seen in some key system characteristics and mission-critical features included to enhance network availability, resilience and security. GSM was originally designed to handle mostly voice traffic, though later updates, such

⁷² GSM is currently the most popular standard for mobile telephony with about 2.5 billion users globally (GSM World 2007).

as General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE), have enabled data services for GSM users. By contrast, TETRA has been defined from its onset (TETRA Release 1) to handle both voice and data traffic. Furthermore, an order of magnitude improvement in TETRA data transfer rates will be enabled by the implementation of TETRA Enhanced Data Service (TEDS) as part of TETRA Release 2 (ETSI EN 2007a). A comparison of the key system characteristics of TETRA and GSM are summarized in Table 6. The comparative advantages of TETRA include:

- Higher bandwidth utilization efficiency.
- Wider coverage possible in the frequency bands allocated for TETRA.
- Faster call setup times, essential in situations that require fast responsive actions.
- Modulation schemes that is relatively simple to implement.
- Cost-effectiveness in serving a low subscriber density.
- Extremely versatile group call functionality.
- Possibility of creating virtual private networks (VPNs) that firmly isolate traffic belonging to different user groups.
- Improved robustness to multipath impairments caused by signal reflections. Diffractions and scattering in the mobile radio environment.

The primary air interfaces (that is, calling modes) specified by TETRA are the Trunk Mode Operation (TMO)⁷³ and Direct Mode Operation (DMO). The TMO is the same as in conventional cellular networks, whereby, users communicate via the TETRA SwMI. On the hand, DMO enables TETRA users to communicate directly or via repeaters, independent of SwMI (see Figure 12). These repeaters are typically vehicle-mounted terminals that improve the DMO range, particularly if the vehicle is parked in an elevated location, such as a hilltop. Furthermore, DMO repeaters may increase range of base stations by providing a DMO link to users that are beyond the coverage range of a base station. See Figure 12 for an illustrative comparison of these different configurations. The use of DMO could be considered as a fallback scheme that ensures continued local communications (with limited features) even after failure to the SwMI.

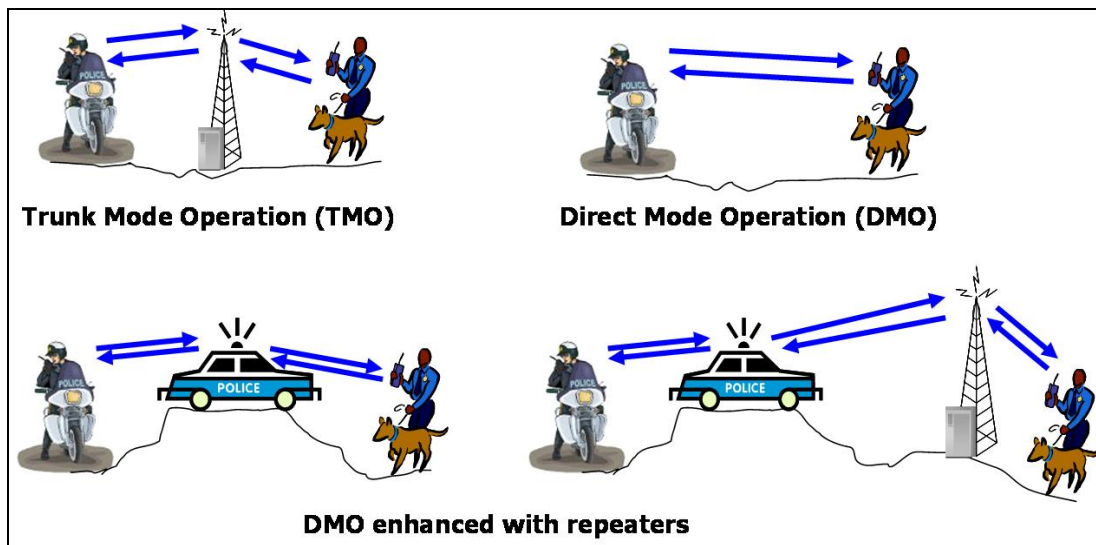
TETRA Services and Applications

TETRA networks support a range of calling features and services crucial for professional users (see Figure 13). This includes not only basic telephony services similar to those provided by public networks, but also a set of supplementary services to increase the effectiveness of teamwork within and beyond a TETRA user group. For instance, during a fire fighting operation a fire fighter may make a Late Entry into a group conversation with other squad members, or a Priority Call from a critically injured fire fighter may override other calls in progress. TETRA also supports standard data services and applications developed by third parties.

⁷³ Also known as the TETRA Voice and Data (TETRA V+D) air interface.

Table III—6 Comparison of key system characteristics between TETRA (Releases 1 and 2) and GSM (Phases 1 and 2).

System Characteristic	TETRA Release 1	TETRA Release 2	GSM Phase 1 and 2
Frequency Bands (MHz)	300-1000	300-1000	900; 1800; 1900
Maximum data rate (kbit/s)	< 28.8	< 538	< 40 (GPRS); < 160 (EDGE)
Maximum mobile speed (km/hr)	200	200	250 (125 at 1800 MHz)
Maximum range (km)	58	83	35 (without extensions)
Channel separation (kHz)	25	25; 50; 100; 150	200
Channels per 200 kHz carrier bandwidth	32	32	8 or 16
Channel access	TDMA	TDMA	TDMA
Modulation schemes	$\pi/4$ DQPSK	$\pi/8$ D8PSK; 4-QAM; 16-QAM; 64-QAM	GMSK
Call setup time (seconds)	0.3-1	0.3-1	4-10
Permissible delay spread (μ m)	100	100	16

**Figure III—12 Basic configuration of various TETRA air interfaces.**

These include the status messages (encoded as 16-bit numbers), Short Data Service (SDS)⁷⁴ and IP data services enabling Internet/Intranet access, file transfer (e.g. fingerprint scan, maps, mug shots, ECG trace etc.), email, database lookups, Automatic Vehicle Location (AVL), telemetry and so forth. Even faster data rates to support rich multimedia services (e.g. streaming video) will be possible with the implementation of TEDS.

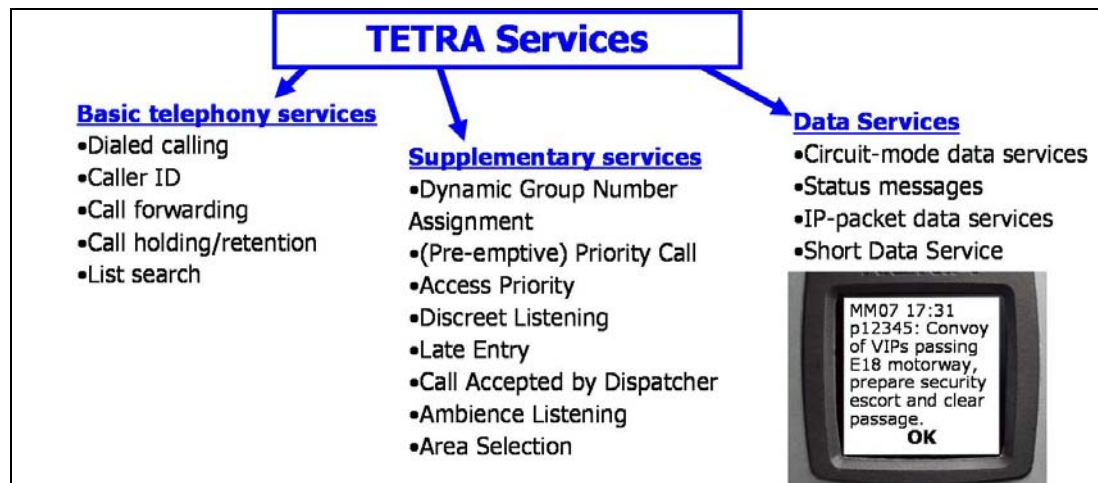


Figure III—13 Typical services for TETRA users. An example screenshot of a Short Data Service message is shown inset.

In addition to these services, TETRA supports three call types: private, group and phone calls (see Figure 14). Group calls are important in fostering team work as they enable a user to communicate instantly with members of their designated group by simply pressing a Push-To-Talk (PTT) on their MSs to initiate the group call or request transmission permission. Members of a closed user group (CUG) typically have their traffic isolated from other users of the TETRA system. Emergency calls are pre-emptive calls that can belong to any of the three call categories, and are usually initiated by pressing a dedicated red button on a user's MS (see Figure 10).

In recognition of the market potential of PMR services, the GSM standard has since been updated with PMR-like features in the GSM Phase 2+ release. The updates include Advanced Speech Call Items (ASCI) that enable GSM networks to support: improved group communications; broadcast and pre-emptive calls; PTT over cellular (PoC) functionality with fast call setup times; and VPNs for group isolation. However, traditional PMR standards (e.g. TETRA, APCO-25) still retain an edge over GSM Phase 2+ due to availability of mission-critical survivability features (e.g., DMO) that are still not available in the latter (TETRA MoU Association 2004). Another GSM PMR standard is the GSM-Railway (GSM-R) standard that was developed specifically for the rail sector under a special agreement with the railway operators. GSM-R includes ASCI functionalities

⁷⁴ SDS bears a close resemblance to the popular Short Message Service (SMS) available in the public mobile communication systems. A basic SDS message contains up to 255 characters, significantly more than an un-concatenated SMS that is limited to 160 characters.

mentioned previously, but requires dedicated base stations deployed every few kilometres alongside rail tracks.

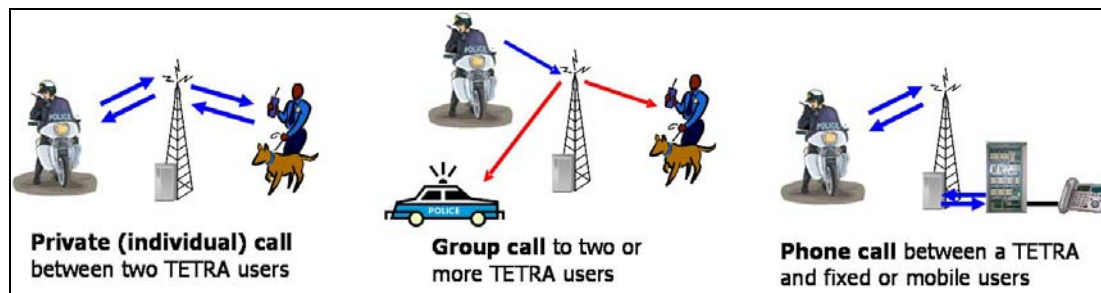


Figure III—14 Three call types supported in TETRA networks.

VIRVE: An Example TETRA Network

VIRVE (VIRanomaisVerkko) is a TETRA network that covers the whole of Finland (330,000 km²) using extensive TETRA infrastructure made of around 1300 BSs and 15 MSCs (see Figure 15). The network coverage area includes the Gulf of Finland for maritime purposes and serves the Estonian frontier guards and maritime agencies. VIRVE is operated by the state-owned State Security Networks Ltd. (Suomen Erillisverkot Oy). The network currently accommodates about 50,000 users belonging to multiple agencies with the actual fraction of each user group shown in Figure 15.

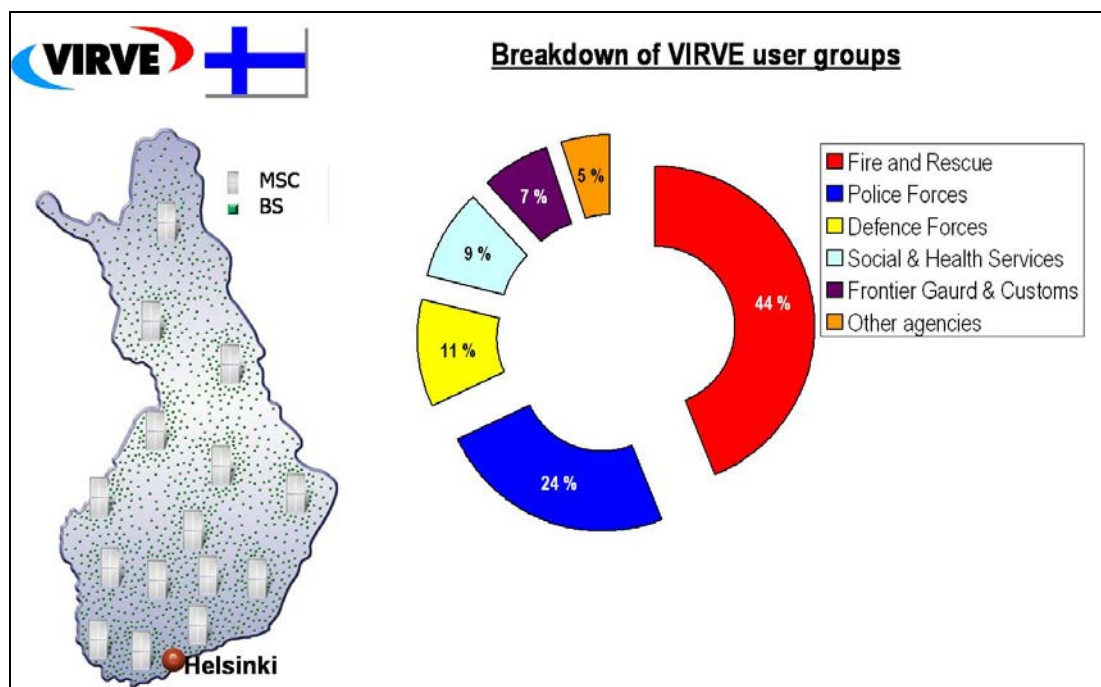


Figure III—15 Positioning of VIRVE TETRA infrastructure and the breakdown of VIRVE user groups. (Juvonen 2005; Vilppunen 2005)

As a shared network, VIRVE enables a more flexible and coordinated response among relevant authorities and agencies when dealing with high-impact events, such as winter storms. However, despite being a common shared network, the

different agencies are afforded the same privacy and resources as they would in dedicated networks, via strong guarantees on data protection and provision of high-speed data services.

Example use of VIRVE is the integration of VIRVE with the 15 Emergency Response Centers (ERC) spread across Finland (Juvonen 2005; Vilppunen 2005). The ERCs receive about two million ambulance police or rescue-related phone calls made by the public to the 112 emergency number and forwards them to the appropriate agency via VIRVE. Another example of the use of VIRVE is by the Radiation and Nuclear Safety Authority (STUK) that has a mission to prevent and limit the harmful effects of radiation. Radiation measurement data is gathered every 10 minutes from around 200 monitoring stations in Finland. This data is then relayed by telemetry modules to STUK and local ERCs via VIRVE using TETRA IP packet data transfer and SDS messaging as backup (Vesterbacka 2007).

Security assessment methodologies

The increased ubiquity, diverse features and functionality of information systems have been accompanied by the increase in complexity of implementing necessary security measures. This has created a need for security frameworks to provide a streamlined way for assessing and analyzing information system security taking into account: threats and attacks, vulnerabilities, and security (detection, correction and prevention) measures. To that end, a range of security assessment methodologies have been proposed, such as the following:

- CORAS: a UML-like model-based method for analyzing threats and risks developed by the EU-funded CORAS project.(CORAS 2006)
- OCTAVE®: “Operationally Critical Threat, Asset, and Vulnerability Evaluation” method is developed by Carnegie Mellon CERT Coordination Centre (CERT 2003).
- STRIDE: “Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Escalation of privileges” method developed by Microsoft (Hernan et al 2006).
- EBIOS: “Expression of Needs and Identification of Security Objectives” method developed by developed by the France’s Central Information Systems Security Division (Central Information Systems Security Division 2005).
- eTVRA: eEurope secure and trusted infrastructure Threat, Vulnerability and Risk Assessment method being developed by Specialist Task Force (STF) 292, associated with Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN) standardization body of ETSI (Judith et al 2007).

The focus of this report is on the assessment methodology based on the ITU-T X.805 security architecture (ITU-T 2003) that was originally developed and presented for standardization by Lucent Technology (formerly known as Bell Labs, now Alcatel-Lucent). The architecture was also later accepted by the International Organization for Standardization (ISO) and the International Electrotechnical Committee (IEC) as the basis of a joint enterprise standard, ISO/IEC 18028-2.77 (ISO/IEC 2005).

Description of ITU-T X.805 Security Architecture

The ITU-T X.805 security architecture provides a comprehensive top-down, end-to-end perspective on network security. It is therefore applicable to assessing the security of the network's infrastructure, services and applications. Moreover, flexibility in the definition of the security architecture enables it to be applied to diverse network types independently of network technology. The security architecture addresses various questions on network protection based on three architectural components: security dimensions, security layers and security planes (see Figure 16).

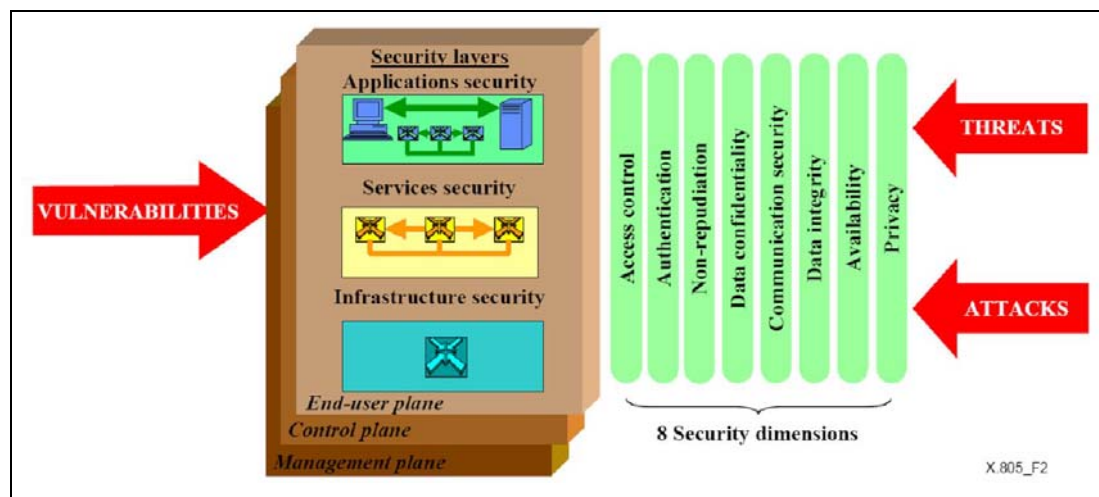


Figure III—16 ITU-T X.805 security architecture for end-to-end network security. (ITU-T 2003)

1. Security dimensions: are measures that address a particular aspect of network security. The eight security dimensions are:

- I. Access control to protect against unauthorized use or tampering of network assets and resources.
- II. Authentication to confirm the identities of communicating entities.
- III. Non-repudiation measures to prevent individual or entity from denying having performed a particular network-related action.
- IV. Data confidentiality to protect data from unauthorized disclosure.
- V. Communication security to ensure information flowing between two points is not diverted or intercepted in transit.
- VI. Data integrity to ensure data correctness or accuracy.
- VII. Availability to ensure that authorized access to network resources is not interrupted by events impacting the network.

2. Security layers: are hierarchies of network equipment and facility groupings upon which the security dimensions are applied. Each Security Layer has unique vulnerabilities, threats, and mitigations. The three security layers are:

- I. Infrastructure security layer constituting network transmission facilities and devices that are fundamental building blocks of the network (e.g., servers, routers, base stations, links between base stations and switching centre).
- II. Services security layer addressing security of services provided by the network (e.g., Internet access services, voice calls, VPN, SDS/SMS messaging).
- III. Applications security layer addressing security of network-based applications accessed by network users (e.g., email, web browsing, file transfer, online training, electronic/mobile-commerce).

3. Security planes: are categories of network-related activities protected by security dimensions. The three activity planes in the security architecture are:

- I. The management security plane concerned with protection of OAM&P functions of network elements, services and application. Includes the fault, capacity, administration, provisioning, and security (FCAPS) functions.
- II. The control security plane concerned with the protection of activities that enable efficient delivery of information, services and applications across the networks. Includes machine-to-machine communication of control or signalling information for configuring devices to route traffic across network.
- III. The end-user security plane addresses security in the user's process of accessing and utilizing services provided by network. This also includes actual end-user payload or data flows (e.g., images, data files, streaming video).

Each of the aforementioned security planes along with the three security layers must be secured to provide an effective end-to-end security posture.

Utilization of the ITU-T X.805 Security Architecture

The ITU-T X.805 security architecture components described previously enable the identification of security issues that need to be addressed in countering threats adopted from ITU-T X.800, namely: destruction, corruption, removal, disclosure and interruption. Table 7 shows the security dimensions and the corresponding security threats that are addressed by each dimension. For instance, the authentication security dimension counters the threat of removal or disclosure of information.

The ITU-T X.805 security architecture enables modular, systematic and organized assessment and planning of network security. Figure 17 illustrates in tabulated form how the intersection of three security layers and three security planes provide nine unique perspectives or modules for consideration of the eight security dimensions. Notably, the security dimensions of different modules would have a different set of objectives and hence different set of security measures. This tabular form provides a convenient way of describing the security dimension objectives for each module.

The objective of each one of the aforementioned modules is summarized briefly in Table 8.

Table III—7 Threats defined in ITU-T X.805 framework and corresponding security dimensions proposed to address them (a thumbs-up sign implies the threat is countered by a security dimension in the corresponding row).

SECURITY DIMENSIONS	SECURITY THREATS				
	Destruction of info & resources	Corruption of info	Removal of info & resources	Disclosure of info	Interruption of services
Access control	👍	👍	👍	👍	
Authentication			👍	👍	
Non-repudiation	👍	👍	👍	👍	👍
Data confidentiality			👍	👍	
Communication security			👍	👍	
Data integrity	👍	👍			
Availability	👍				👍
Privacy				👍	

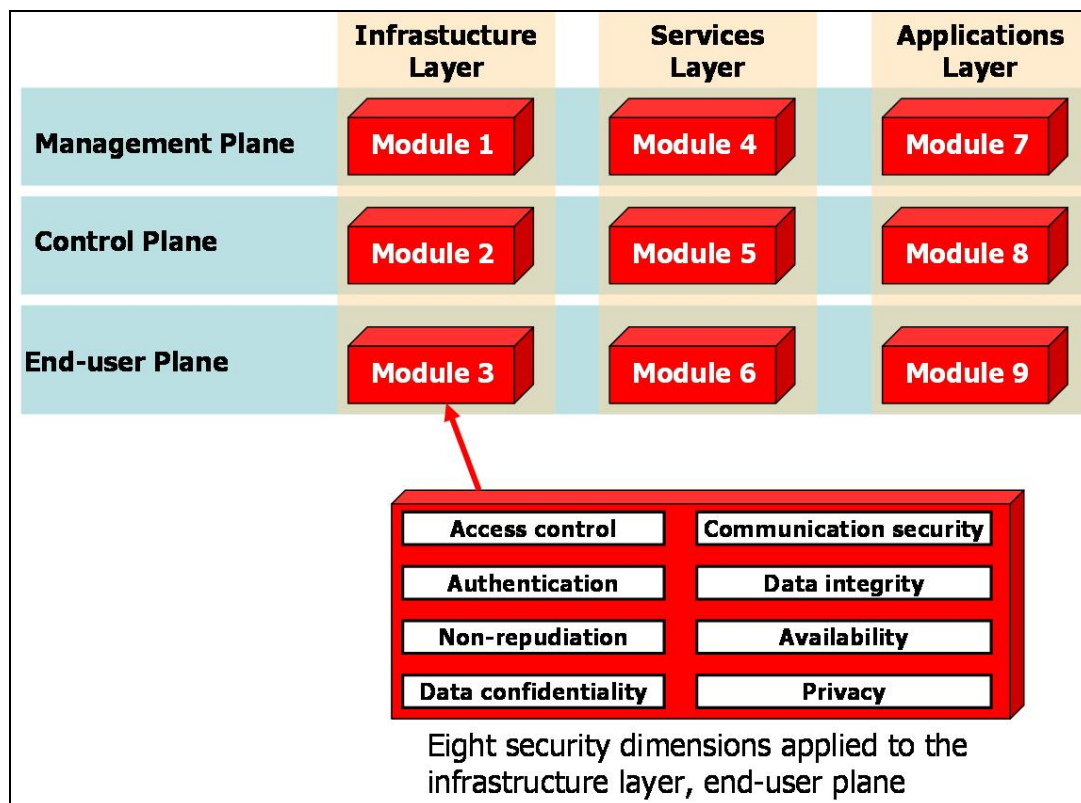


Figure III—17 Nine unique perspectives or modules of the ITU-T X.805 security architecture.

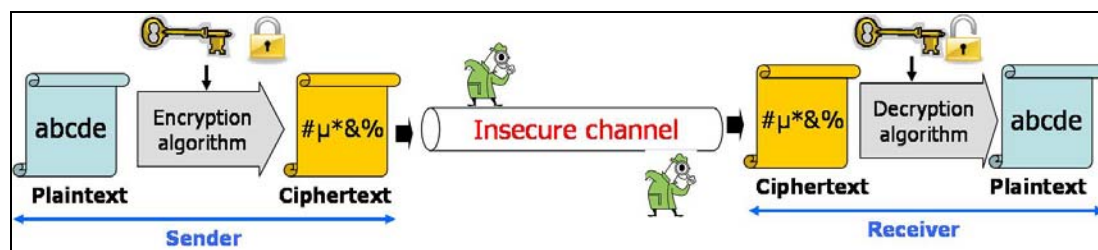
Table III—8 Security objectives of the nine unique modules of the ITU-T X.805 security architecture.

Module	Security Objectives
Module 1: Infrastructure layer, management plane	Securing OAM&P of individual network elements, communication links and server platforms that constitute the network.
Module 2: Infrastructure layer, control plane	Securing control or signalling information residing in network elements and server platforms.
Module 3: Infrastructure layer, end-user plane	Securing user data and voice that is stored or being transported through network elements.
Module 4: Services layer, management plane	Securing the OAM&P functions of network services.
Module 5: Services layer, control plane	Securing control and signalling information used by the network service.
Module 6: Services layer, end-user plane	Securing user data and voice as it uses the network service.
Module 7: Application layer, management plane	Securing OAM&P functions of a network-based application.
Module 8: Application layer, control plane	Securing the control or signalling information used by network-based applications.
Module 9: Application layer, end-user plane	Securing user data (e.g., user's credit card number) provided to the network-based application.

Security posture of TETRA networks

Security Aspects Addressed in TETRA Standards

The TETRA standards define a wide range of security measures, most of them being based on cryptography techniques (ETSI EN 2007a). Encryption enables secure communications over an otherwise insecure channel being monitored by potential eavesdroppers. This is implemented by using an encryption algorithm and a secret encryption or cipher key at the sending side to encrypt plaintext (original message or data) into unintelligible cipher text that is then transmitted over the insecure channel (see Figure 18). A reverse process is carried out at the receiving side, whereby the original plaintext is recovered from the cipher text using the correct key and decryption algorithm. Apart from providing encrypted communications, the encryption keys can be used for one-way or mutual authentication between sender and receiver (typically under a public key infrastructure or PKI arrangement) before any user traffic is sent.

**Figure III—18 Basic steps taken in encrypted communications.**

The Security and Fraud Prevention Group (SFPG) of the TETRA MoU Association is tasked with updating the TETRA authentication algorithms (TAA) and TETRA encryption algorithms (TEA) defined for TETRA standards.⁷⁵ TETRA networks usually implement air interface encryption (AIE) between MS and SwMI (see Figure 19). The AIE keys may be derived dynamically for every authentication procedure, sent to individual MSs or CUGs using Over The Air Re-keying (OTAR), or preloaded (static) in the terminal or subscriber identity module (SIM). Furthermore, end-to-end encryption (E2EE) may be used to provide encryption within the SwMI for more robust security (see Figure 19), for instance, over third-party leased copper lines used on a BS-to-MS link. The key management for E2EE is provided by Over The Air Keying (OTAK) mechanisms.

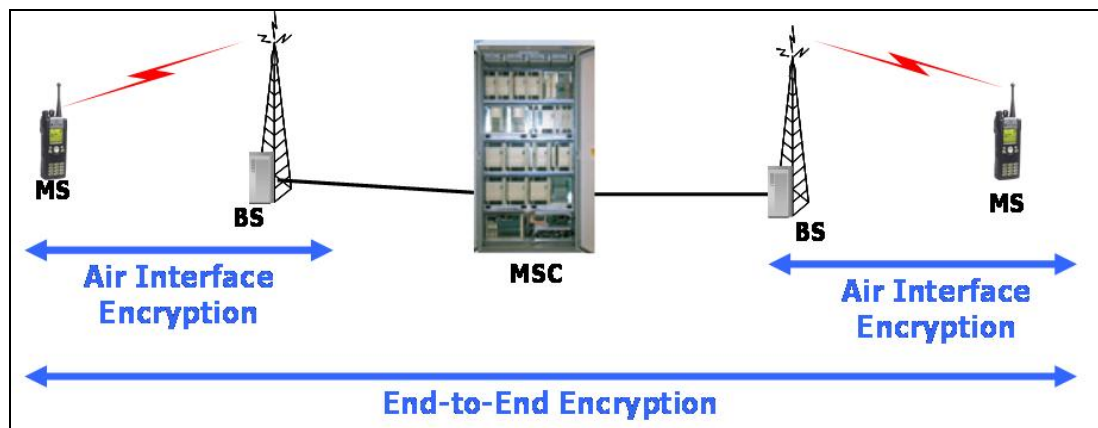


Figure III—19 Implementation regions for air interface and end-to-end encryption schemes.

The TETRA standard defines three security classes depending on the usage of authentication, encryption and OTAR key management (see Table 9). An MS may support one, two or all security classes. Mission-critical PSS TETRA networks such as VIRVE would normally employ the most robust (Class 3) security level.

Table III—9 Security classes defined by the TETRA standards.

Security Class	Authentication	Encryption	OTAR
Class 1	Optional	E2EE (optional); AIE (none)	None
Class 2	Optional	E2EE (optional); AIE using static key encryption (mandatory)	Optional
Class 3	Mandatory	E2EE (optional); AIE using dynamic key encryption (mandatory)	Mandatory

The MS provides users with access to the TETRA network. Therefore, the possibility of threat actors obtaining unauthorized access via stolen or lost

⁷⁵ Some of the TEAs used by European agencies face strict export control for usage in countries outside the Wassenaar Arrangement (2007).

terminals, and the existence of rogue or negligent users, poses significant security threats. TETRA standards define mechanisms for remotely disabling compromised MS equipment (disabling Terminal Equipment Identity, TEI) or MS subscription (disabling Individual TETRA Subscriber Identity, ITSI) by the SwMI. An MS moving from DMO to TMO, or from TMO to DMO retains its disabled state to prevent attempts by the disabled MS to switch to DMO. Subsequently, the terminals may be re-enabled if recovered by the responsible organization. The use of authentication is embedded in the MS disable/enable mechanisms to ensure that the correct MS is disabled or enabled by a legitimate SwMI.

Network Survivability Mechanisms

Network survivability refers to the ability of the network to continue providing a service regardless of component failures within the network infrastructure. Mission-critical systems such as TETRA networks incorporate survivability strategies to mitigate the impact of failures within the SwMI. The strategies employed are likely to differ from one operator to another depending on the equipment they use, as each vendor incorporates different proprietary solutions for survivability in their equipment. Failures in the TETRA network may occur at different locations due to various reasons. The shadowing effect (of buildings, mountains) and failure of one or more components within a TETRA BS may result in partial or full service loss within a cell. Furthermore, the link between the BS and MSC may be lost (e.g., due to a cable cut) leaving the BS disconnected from the rest of the SwMI. Failures of internal MSC components that may result in the partial or complete failure of an MSC are even more detrimental as this may affect multiple BSs connected to the MSC.

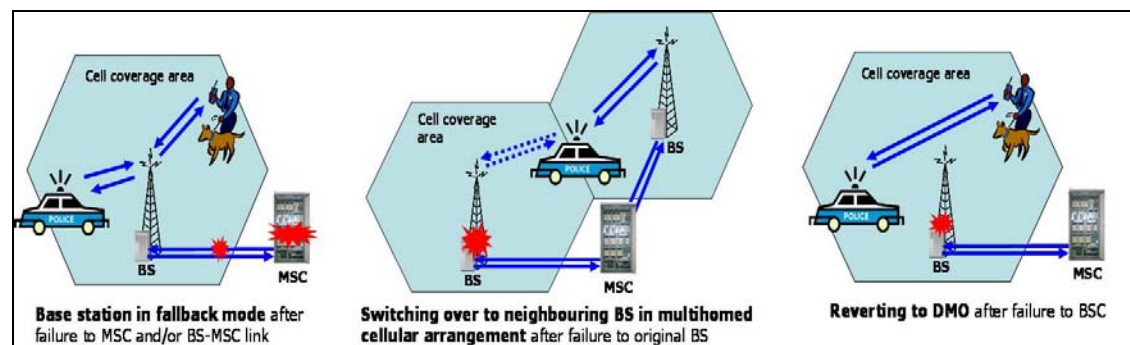


Figure III—20 Possible TETRA network survivability mechanisms based on base station fallback mode, DMO and multihomed cellular network arrangement.

The likelihood of a BS or MSC failing could be reduced by installing redundant components in vacant slots on the equipment racks. The redundant components could then immediately take over operations (automatic failover) if one of the components they backup fails. Decisions on how much redundancy is required should be balanced against the increased capital and operational costs that come with the redundancy. Alternatively, recovery mechanisms could be carried out by reconfiguring the network in the case of the failure of a BS, MSC or BS to MSC link. Base station fallback mechanisms could be employed if the connection to the MSC is lost or the MSC fails, with the BS functioning as a repeater in the cell

coverage area (see Figure 20). If the BS fails, users may either revert to DMO or access the BS of an adjacent cell (fallback mode) under multihomed cellular arrangement (see Figure 20).

Another potential failure scenario is the loss of BS-to-MSC and MSC-to-MSC links. These links are typically implemented using wire line (e.g., fiber) or fixed wireless (e.g., terrestrial microwave) technologies. Failure of any of the links would also result in major service disruptions, such as loss of connectivity between two major cities due to loss of a MSC-to-MSC link. Various network protection mechanisms usually employed to ensure link survivability. These mechanisms require analysis of different failure scenarios during the planning phase, advance allocation of spare capacity for service restoration and distributed recovery to enable rapid service restoration. An example of MSC-to-MSC instant (sub 60 ms) link recovery method using a SDH (Synchronous Digital Hierarchy)⁷⁶ ring topology is shown in Figure 21. Under normal operating conditions, traffic is routed directly between MSC 3 and GMSC (see Figure 21). However, in the event of a failure (in this case a fibre cut), the SDH node connected to the GMSC automatically switches to the duplicate traffic sent on the protection fibre configured in the opposite direction of the ring.

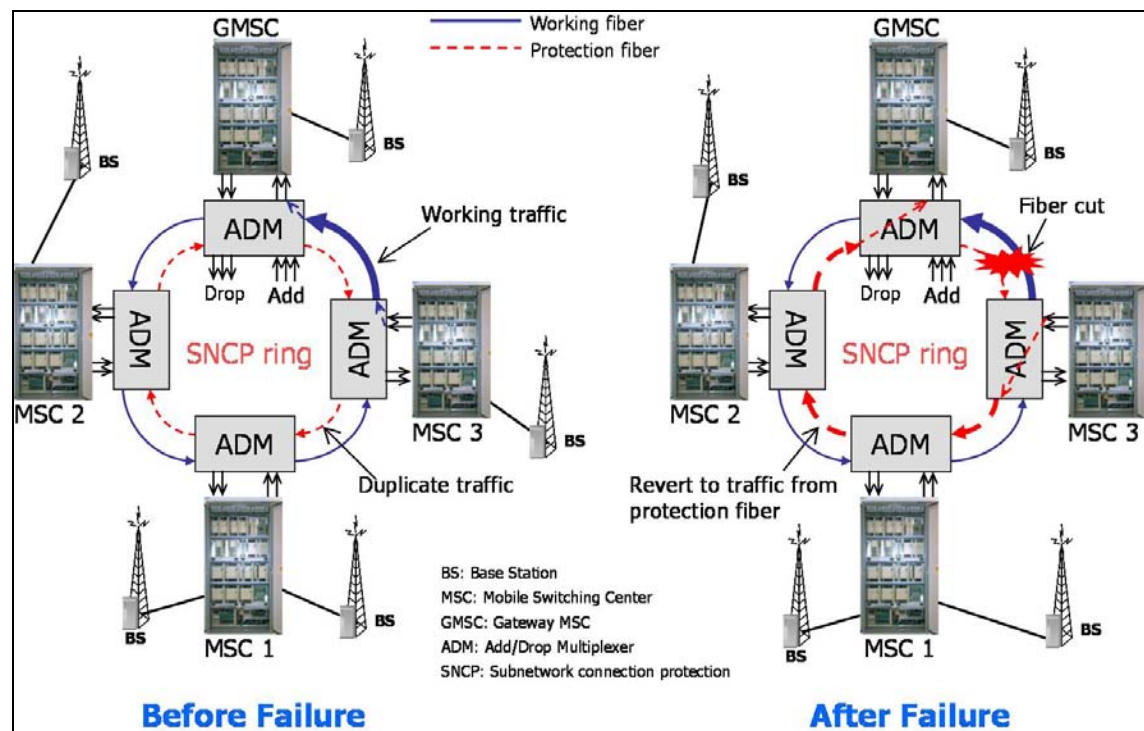


Figure III—21 Example recovery of the link between MSC 3 and GMSC using a resilient four node SDH ring topology.

TETRA network also includes user databases that support user and service mobility. These databases include the TETRA Equipment Identity (TEI) register,

⁷⁶ SDH is the commonly used standard for fixed transmission and multiplexing of high speed signals. The SDH standard defines various survivable network topologies (e.g., point-to-point, ring, mesh etc.) that are resilient to failure.

location registers and authentication centre (AUC) that need to be protected. For instance, a failure of the AUC may result in the loss of call setup capabilities. Survivability of databases may be implemented by switching over to standby databases that are continuously updated with data from the primary databases.

Security and Protection of Physical Infrastructure

Security measures are also essential to prevent unauthorized physical access by potential threat actors to equipment at TETRA cell tower sites, MSC facilities and Command & Control Centre premises. Intruders can be kept away from these locations by using perimeter fences topped with barbed wire, cages, bomb-proof buildings, bunkers, solid steel doors and so forth. Moreover, security of the infrastructure locations can be enhanced round-the-clock monitoring using remote surveillance using CCTV cameras or by having security personnel physically present at the locations. The former is more suitable for cell site surveillance due to the relatively large number cell sites typically present in a network. The aforementioned measures also address the security of the network operations personnel based in those locations. Further protection is also provided against man-made and natural hazards by reinforcing telehousing facilities, fitting smoke detectors, temperature sensors, air filtering systems, flood proofing and providing back-up battery power.

TETRA assessment using ITU-T X.805 security architecture

This subsection assesses typical TETRA network security features and protection mechanisms, using the modular approach of the ITU-T X.805 security architecture. This is not meant to be an exhaustive listing of security features or a TETRA network, but rather indicative of some of the common security measures that could be undertaken by an operator. It should be noted that some of the security measures are interdependent, and may have some overlapping functionality.

Modules 4 to 6

The TETRA network's service layer security measures addressed in the management, control and end-user planes (Modules 4-6) are summarized in Table 11.

Modules 1 to 3

The TETRA network's infrastructure layer security measures addressed in the management, control and end-user planes (Modules 1-3) are summarized in Table 10.

Modules 7 to 9

The TETRA network's application layer security measures addressed in the management, control and end-user planes (Modules 7-9) are summarized in Table 12.

Table III—10 TETRA network security measures addressed in Modules 1-3 of the ITU-T X.805 security architecture.

Module	Security Measures
Module 1: Infrastructure layer, management plane	• Only authorized personnel with administration rights granted access to element or network management systems to perform network management activities remotely or via a craft port • Maintenance of a log (e.g., system log, audit trails etc.) of all management actions or events • Protection of configuration information and administrative IDs/passwords from unauthorized viewing, diversion, deletion or modification • OTAR and/or OTAK secure encryption key management • Backup content and protect connectivity to user management databases
Module 2: Infrastructure layer, control plane	• Error-correction coding⁷⁷ to ensure the correct delivery of information carried over the control channel⁷⁸ • Encryption of signalling information over the air interface (AIE) • Archive recording of all control room traffic for later playback • Protection of fixed signalling network links
Module 3: Infrastructure layer, end-user plane	• Error-correction coding to ensure the correct delivery of information carried over the traffic channel⁷⁹ • Compression and protection of user speech traffic by using speech encoding⁸⁰ • One way and/or mutual authentication between the MS and SwMI, to verify the terminal and legitimacy of the network • Remotely disabling of compromised MS equipment or subscription • User logon by keying in a Personal Identification Number (PIN) or sending a Radio User Identity (RUI)

⁷⁷ Error correction codes employed in TETRA systems include block codes, rate-compatible punctured convolutional codes (for phase modulation) and turbo codes (for QAM). See also ETSI EN (2007b) and ETSI TR (2007).

⁷⁸ TETRA's control channel (CCH) is used to carry signalling messages and packet data (ETSI EN 2007b).

⁷⁹ TETRA's traffic channel (TCH) is used to carry speech and circuit-switched data (ETSI EN 2007b).

⁸⁰ TETRA networks use Algebraic Code Excited Linear Prediction (ACELP) encoding. TETRA Air Interface (ETSI EN 2007b). See also ETSI TR (2007).

Table III—11 TETRA network security measures addressed in Modules 4-6 of the ITU-T X.805 security architecture.

Module	Security Measures
Module 4: Service layer, management plane	• Rights to administer and manage services (e.g. management of group membership) restricted to dispatch and network administration personnel. • Maintenance of a log of service administrative and management actions or events. • Protection of service configuration, management and administrative information. • Backup content and protect connectivity to user service databases. • Protect identity of users, user groups and terminals (e.g., TEI, ITSI, GTSI etc.) utilizing a service. • Maintenance of user activity log containing information terminal. enabling/disabling, location updates vs. time, Call Detail Records (CDR), supplementary services invoked and so forth. • Recovery mechanisms for component or link failures causing service loss.
Module 5: Service layer, control plane	• Encryption of service control information transported within the network. • Error-correction coding to ensure the correct delivery of service control information. • Continuous monitoring and control of user calls.
Module 6: Service layer, end-user plane	• Restrict service usage (e.g. by checking subscription rights) to only authorized users, user groups and terminals. • Encryption of user traffic being transported by service over the air interface and/or end-to-end. • Protect user IP services against DoS attacks (e.g., using firewalls, IPSec etc.) • Retain records of recent service usage history in user terminal. • Jamming detection and countermeasures (e.g., switching to a different frequency) to prevent service loss.

Table III—12 TETRA network security measures addressed in Modules 7-9 of the ITU-T X.805 security architecture.

Module	Security Measures
Module 7: Application layer, management plane	• Rights to administer and manage applications restricted to authorized personnel, application providers and terminals. • Protect files used in the execution and creation of applications (e.g., executable files). • Protect identity of users, user groups and terminals (e.g., TEI, ITSI, GTSI etc.) utilizing an application. • Maintain a database of applications accessed and utilized by users, user groups and terminals.
Module 8: Application layer, control plane	• Encryption of application control information transported within the network. • Ensure application control information originates from authorized source.
Module 9: Application layer, end-user plane	• Protect identity of users, user groups and terminals (e.g., TEI, ITSI, GTSI etc.) utilizing an application. • Encryption of user traffic (e.g., patient's ECG trace) being transported over the air interface and/or end-to-end. • Protection of application files/data using conventional methods (e.g., email and attachments using PGP, S/MIME etc.). • Restrict access and use of applications (e.g. using passwords) to authorized users, user groups and terminals.

Example TETRA traffic analysis

One of the key measures in ensuring service availability for critical missions in TETRA networks is to consider some of the likely scenarios right from the planning stage. As an example, we present some simplified traffic analysis that could enable networks planners to make key decisions on how to manage limited resources (channels) under various operating conditions.

The call setup time (or delay) is one of the important TETRA performance parameters, particularly in moments during or immediately after a crisis, where the requirement for split-second decisions and responses is high (Rantanen 2003). In cases of extreme load because of many simultaneous callers the call setup time tends to increase because of the higher contention for resources. At that point dispatchers will start prioritizing calls by queuing, blocking or dropping low priority calls and giving preference to high priority calls.

Consider a service area that has the following TETRA user groups:

- Police: twenty traffic police officers working in pairs and five groups of security police each with of five members.
- Fire Brigade: four units each consisting of five fire fighters.
- Ambulance: six ambulance units of each with a crew of three (1 driver and 2 paramedics).

Furthermore, the following assumptions are made about the calls made by the different groups in the service area, under normal (crises-free) operating conditions:

- Roughly the same traffic type generated by all groups.
- All user groups receive hourly alerts or urgent messages from the dispatcher.
- All user groups report incidents as they occur.
- Average call length is 30 seconds and the average call volume of two call attempts per group per hour.
- Two call setup time limits are considered, 0.5 seconds or less being the favourable delay, and 10 seconds being the least favourable time, beyond which the call is dropped.
- The service area is covered by 4 TETRA BSs, each with one carrier (4 time slots).
- BSs are deployed in a multihomed arrangement that enables continuous service even if only one BS is left in the area.

In case of crises within the service area (e.g., hurricane), extra staff (police, medical staff, fire fighters) are called to duty. We then assume under these circumstances the number of users is doubled, as is the traffic generated by each user. The dispatcher would manage the situation by assigning the new users to existing groups so as to minimize the number of individual alerts. We evaluate the performance of the network using the Erlang C model, which gives the probability estimate for a call being queued for a particular time before it is established. In Figure 22, it is seen that under normal conditions the probability of calls being queued is negligible. At the moment of crisis, about 2.3% of the calls are queued more than 10s. However, with proper crisis management by the dispatcher some of low priority calls could be blocked and hence only about 1% medium or high priority calls would have to be queued for more than 10s.

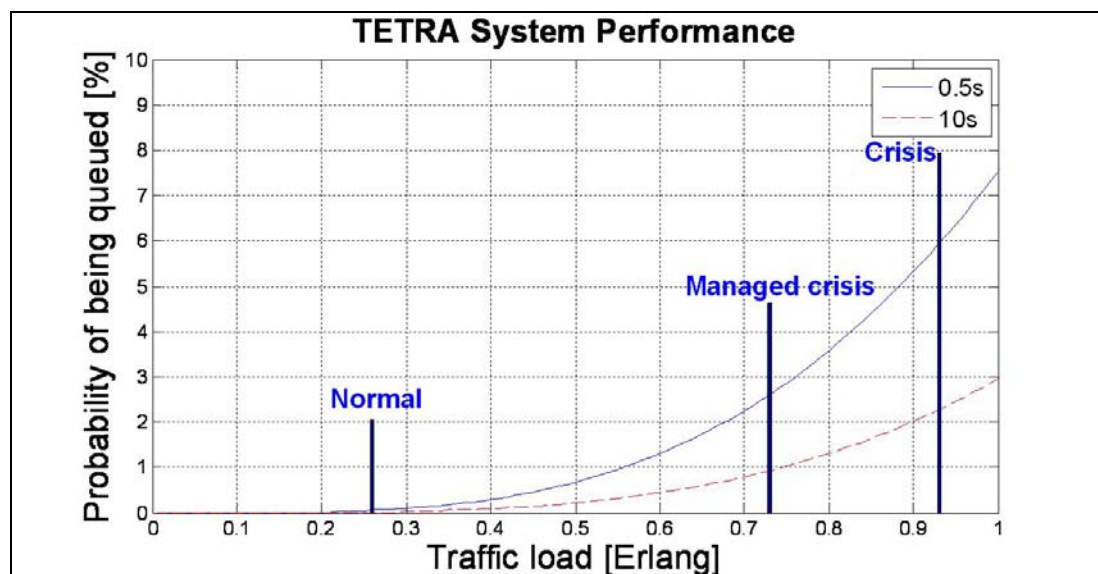


Figure III—22 TETRA system performance under various operating conditions.

To further compound the crises, we assume that some of BSs are damaged as part of the common-cause failures resulting from a hurricane. This means that a larger number of users called in to respond to the crises have to perform their duties using relatively fewer network resources than those available under normal conditions.

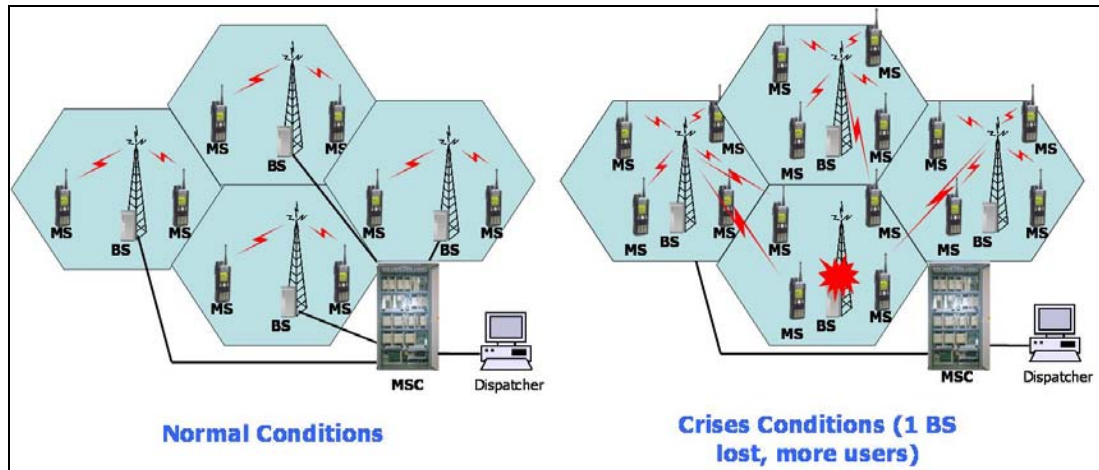


Figure III—23 Available base stations under normal and crisis conditions.

If one BS is lost in a hurricane, the number of calls being queued for more than 10s under crisis management increases to 2%. However, if two BSs are lost during the crisis, the latter figure rises to over 8%, whereby, only 82% of queues can be setup within the 0.5s limit. This implies that the higher the level of disruption of the infrastructure, the more the need for stringent crisis management.

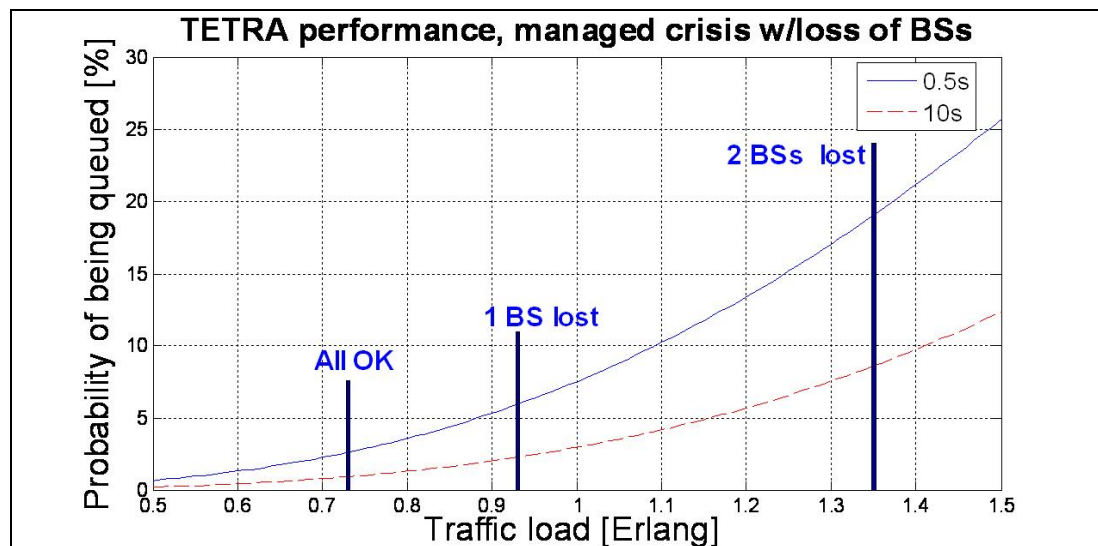


Figure III—24 TETRA system performance under crisis management in various levels of infrastructure disruption.

3.3 COMPREHENSIVE STRATEGY FOR CIIP

The challenge of CIIP has garnered sufficient attention to warrant high level research and in-depth studies by government, businesses, industry experts and academia. This work has resulted in some early understanding of the concept of CIIP and the possible scope of its challenge, as illustrated by the International CIIP 2006 Handbooks (Abele-Wigert and Dunn 2006; Dunn and Mauer 2006). The CIIP challenge stems from the fact that CIIP strategists are usually faced with an abundant and diverse set of complex interdependent scenarios. This may leave different strategy-makers lacking clarity and coherence in achieving what are usually common CIIP goals. Moreover, it increases the likelihood of wasting resources, time and effort by focusing on imperfectly perceived alternatives. The worst-case scenario is of different groupings (private, public or a combination of both) developing different, contradictory and ineffective responses to a universal CIIP challenge. A comprehensive strategy for CIIP aims to avoid those pitfalls by providing CIIP implementers with coherent direction, guidance and focus when faced with a multitude of complex choices.

Strategy is in general a rather elusive and abstract concept. The difficulty in formulating a CIIP strategy is further accentuated by the continuous infrastructure scalability, rapid evolution and constant diffusion of innovations within the information infrastructure. Such a fast-paced technological environment necessitates strategy that is both dynamic and adaptable to changes that occur regularly over time (Duke Corporate Education 2005). Future strategy tends to build upon existing CIIP goals (the end result) and strategy (the means to an end). Figure 25 depicts how a shift in priorities of different groups may force a change in goals and strategy, and how these are then mapped to different dimensions of each group. This strategic context enables a greater sense of purpose by linking activities of different groups to the bigger picture of CIIP. The next subsections provide an overview of strategy within the different CIIP dimensions shown in Figure 25.

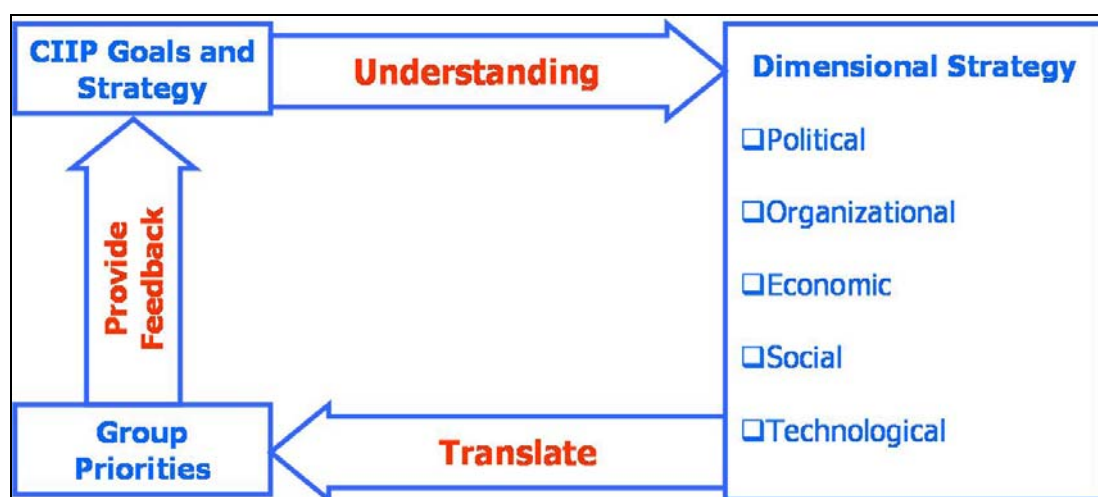


Figure III—25 Continuous lifecycle of strategy on CIIP.

Political dimension

Policies have traditionally resulted from governments' decision to act (or not to act) upon a certain issue, typically in the interest of the general citizenry. For instance, Jenkins defines policy as "a set of interrelated decisions taken by a political actor or group of actors concerning the selection of goals and the means of achieving them within a specified situation where those decisions should, in principle, be within the power of those actors to achieve" (Jenkins 1978). Rauscher extends the definition of policy to include agreements, standards, policies, and regulations, as well as the framework within which different actors interact (Rauscher et al 2006). The US government was one of the first public institutions to formally address the challenge of CIP and developed a national protection strategy under the auspices of the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996 (Executive Order 1996). The efforts of the PCCIP and subsequent commissions resulted in key government policies on CIIP outlining a range of underlying factors (e.g., organizational, legislative, regulatory).

The CIP/CIIP initiatives pioneered by the US government have since been adapted in other countries, albeit with varying interpretations of the challenge and recommended approaches. These differences are clearly noticeable in Volume I of the International CIIP 2006 Handbook that collates a survey of the CIIP policies of 20 countries (Abele-Wigert and Dunn 2006).⁸¹ Moreover, the cross-sector nature of CIIP has meant that multiple agencies (public security, emergency, law-enforcement etc.) working under the same government have tackled the issue of CIIP from different vantage points, with each introducing unique perspectives on the CIIP policy-making process. Abele-Wigert identifies the co-existence of technical (system-level), business, law-enforcement and national security perspectives on CIIP in most surveyed countries, though the prominence of a particular perspective may vary from country to country (Abele-Wigert 2006). Furthermore, the author notes that applying a holistic approach in CIIP policy making would result in policy that is more effective than the one resulting from sum of the individual perspectives (Abele-

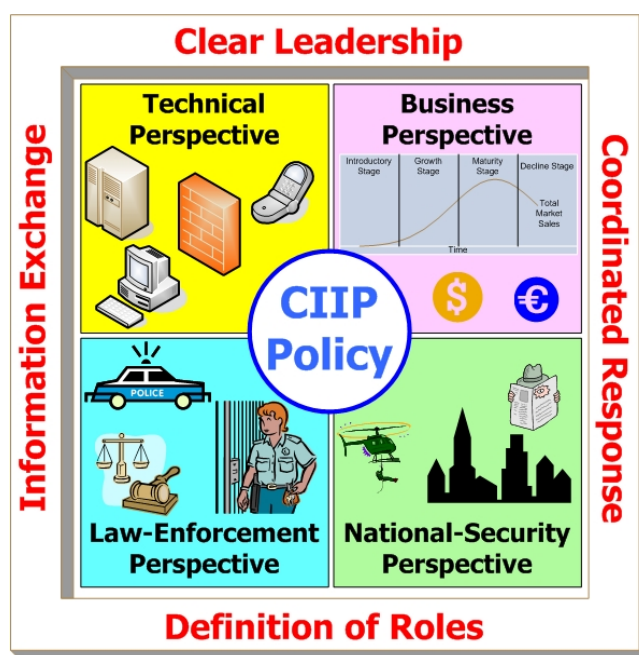


Figure III—26 A holistic approach to CIIP policy making.

⁸¹ The survey includes profiles of CIIP policies from three BSR countries: Sweden, Finland and Germany.

Wigert 2006). The holistic approach is visualized here in Figure 26, whereby multiple perspectives combine to produce common CIIP policy, within an agreed framework of leadership, interaction, coordination and distribution of responsibilities.

Organizational/institutional dimension

The actor groups or organizations that have a stake in CIIP strategy tend to be diverse due to the cross-sector presence of ICT. These organizations may belong to any one of the following groupings:

- Public sector organizations: comprising the government departments and agencies with the responsibility for ensuring overall safety and security, continuity in the delivery of essential services and maintenance of a well-functioning economy. Example agencies in Finland whose interests are aligned with CIIP objectives are: the Finnish Communications and Regulatory Authority (FICORA); the National Emergency Supply Agency (NESA); and the Steering Committee for Data Security in State Administration (VAHTI).
- Private sector organizations: including information infrastructure owners and operators, information and telecommunication equipment manufacturers and vendors, IT security solution providers, service providers, application developers, network planners and systems integrators, and enterprises of all sizes whose processes are heavily dependent on the use of ICT solutions and services.

A key factor that strongly influences CIIP strategy revolves around the ownership and operation of the CII. In recent times the trend of privatizing critical (information) infrastructure in free market economies⁸² has seen an increased transfer in ownership from the public sector (government) towards the private sector (business).⁸³ Furthermore, deregulation measures widely adopted within the ICT sector in the previous decade, have relaxed government restrictions resulting in increased competition, higher efficiency, cutting-edge innovations, affordable services for users, and bumper profits for ICT companies. Therefore, the private sector organizations are now relatively better positioned from a financial, technical and operational standpoint to carry out the practical implementation of various CIIP measures.

Private sector organizations are now undergoing significant changes through strategic actions, such as, consolidations and spin-offs, value chain unbundling and business process in/outsourcing, alliances and joint ventures, and relocation to favourable environments. Furthermore, by adopting ICT solutions and embracing the Internet, more straightforward and value-added ways of interaction have become possible,⁸⁴ resulting in a range of entirely new business models (Davenport and Short 1998). These actions are not limited to the private sector, as

⁸² Majority (if not all) of the BSR countries possess strong market economy traits.

⁸³ There are few exceptions to the rule, most notably in the ownership and operation of national PSS networks by governments in the BSR.

⁸⁴ These private sector interactions include B2B, B2C/C2B, B2G/G2B and C2C interactions, where B stands for Business, C stands for Customer and G stands for Government.

public sector organizations are also adopting ‘business process re-engineering’ with the aim of minimizing public expenditure, increasing operational efficiency and improving public services (Anderson 2002; Traunmüller and Lenk 2002). Collectively, these strategic actions create a complex set of relationships that not only exist beyond the ICT sector, but also transcend national borders. Consequently, a new operating environment has emerged, obliging organizations to compete, cooperate, or do both concurrently, whilst adapting to dynamic market trends and shifting incentives. This is illustrated by (but not limited to) the examples below, selected from organizations in the ICT sector.

- Example 1: A wide area fixed network operator who leases bandwidth from a competing operator in areas not covered by their infrastructure footprint, and vice versa. This affords both operators large footprint without the required deployment efforts (ITU-T 2003).
- Example 2: Competing mobile operators who opt (or in some cases, obliged by regulations)⁸⁵ to formulate cell site-sharing agreements with competitors, so as to reduce the total cost of ownership of the infrastructure, speed up network roll-outs and reduce visual pollution by limiting the number of antenna towers.
- Example 3: Non-ICT utility companies who deploy information infrastructure alongside their own infrastructure, so as to generate extra revenue streams to supplement income from their core activities. For instance, the Corenet Oy operates a 5800 km network of telecommunication cables deployed alongside the Finnish VR rail network. Another example is Imatran Voima Oy that has deployed telecommunication cables on the pylons of its Finnish power transmission network. This ‘dual personality’ implies that the utility company may be engaged both as a CI and CII owner.

In the context of CIIP, the net result of this intense restructuring within the ICT sector and the shifting or blurring of both the organization and sector boundaries is the development of even more complex interdependencies. This inevitably leads to an increased vulnerability to threats (de Bruijne and van Eeten 2007), and presents inherent challenges in modelling and analyzing CIIP (Weijnen 2007). To better visualize the role of technology in an organization and its relevance to CIIP strategy, we derive a simplified organizational model that adapts select features from three previously proposed models, namely: the University of Southern California’s Institute of CIIP (ICIIP) Model (Kiely and Benzel 2006), the 4-Layer CIP Model (Reinema 2004) and Galbraith’s Star Model (Galbraith 2007). Our organizational model (see Figure 27) takes the shape of a 3D pyramid (similar to the ICIIP Model) and includes four nodes or key elements: physical and technology elements; people; organizational strategy and structure; and

⁸⁵ The argument for infrastructure sharing is supported by many studies. For example, EUTELIS (1998) produced a report on “Recommended Practices for Collocation and Other Facilities Sharing for Telecommunications Infrastructure” to the National Regulatory Authorities (NRAs) in December 1998. Such recommendations have led to the inception of mobile virtual network operators and switchless operators that offer services even without owning any network infrastructure.

organizational processes. All the nodes are tightly interconnected by organizational intradependencies, whereby significant change or disturbance in any node (such as, changes that affect security e.g., attacks on physical elements, staff cuts, technology upgrades etc.) distorts the overall shape of organizational model. Therefore, for the organization to retain its shape, simultaneous changes are necessary in other nodes to compensate for this initial change.

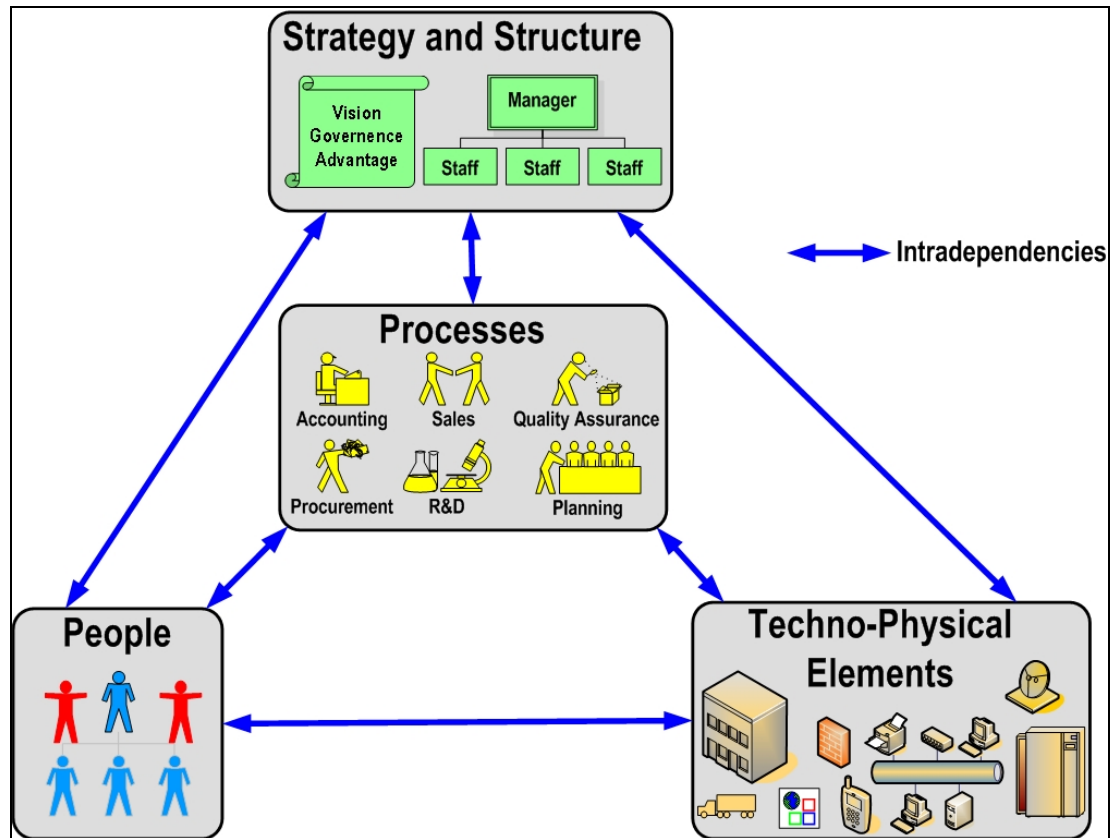


Figure III—27 Four node organization model and its intradependencies.

From the point of view of information security, most organizations now implement and maintain a diverse set of information security controls that span all the four nodes of Figure 27. These controls are amalgamated under some formal information security management (ISM) system. ISM systems are well established as an integral component in most organizations and a range of standards have been published to guide their implementation (Kenning 2001).⁸⁶ The primary focus of ISM tends to be more inward-looking, by putting an emphasis on the intradependencies within an organization, and treating the interdependency with nodes belonging to other organizations as a secondary issue. By contrast, CIIP objectives have a broader scope, placing equal emphasis on both intradependencies and interdependencies associated with a particular organization.

⁸⁶ An example ISM standard is the tripartite BS 7799 standard that was developed in the early 1990s in response to demand from private and public sector organizations for a common information security framework. The standard initially published by the British Standards Institute, has since been internationalized as the ISO/IEC standards 27001 and 27002.

Interdependencies are particularly strong for CII, as they have more prominent ICT constituents that tend to be highly networked (that is, cyber interdependency).

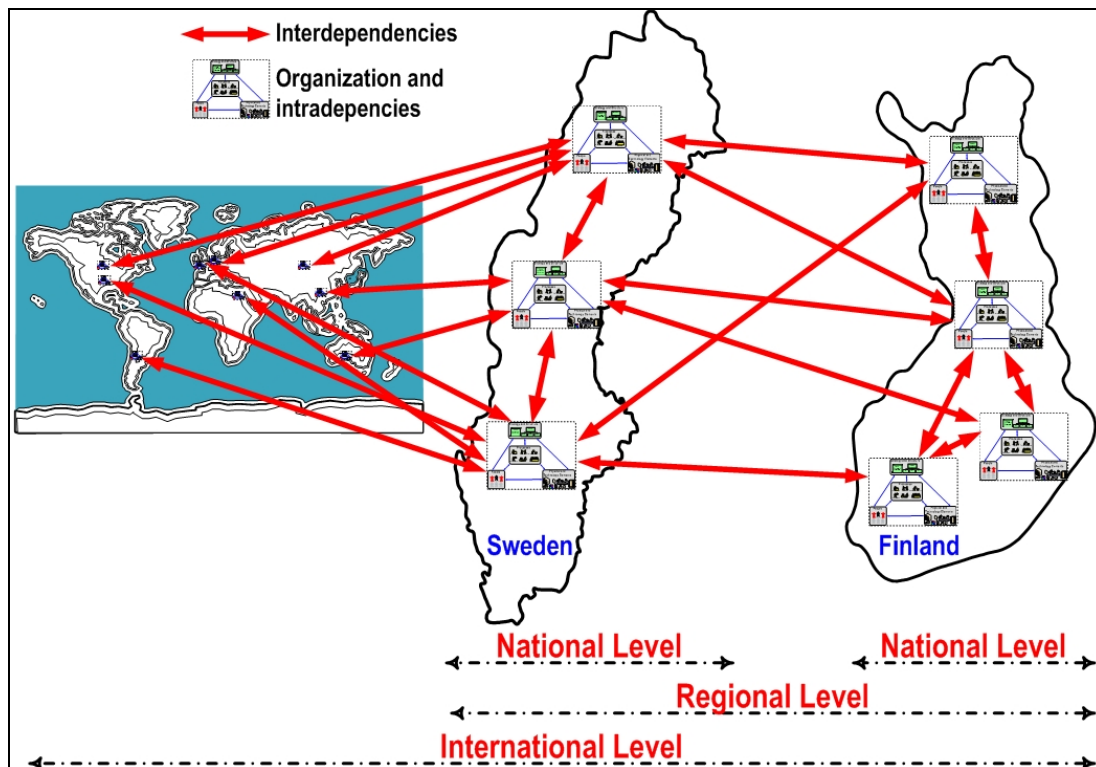


Figure III—28 Organizational interdependencies that may exist at national, regional and international levels.

The unexpected but high-impact threats considered in CIIP possess both a local and global dimension, necessitating the requirement to understand the complex, multidimensional and sometimes deep interdependencies that may exist between organizations at national, regional and international levels (see Figure 28). This understanding enables CIIP planners to foresee how disruptive events could potentially propagate through multiple organizations, and also assist them in identifying critical nodes. However, several developments are needed for CIIP to reach the practical level of maturity attained by ISM practices (Bailas 2006). Among other things, this demands the publication of internationally agreed CIIP standards and best practices, the planning of unlikely but realistic scenarios for emergency preparedness exercises, and the design of computer-aided tools for (intra)interdependency simulations, decision support, crisis management, and so forth.⁸⁷

Against the background of these organizational changes and interdependencies, governments are expected to provide a secure and conducive operating environment for businesses, unbiased leadership, as well as authority for

⁸⁷ ISM practitioners currently have a wide range of tools at their disposal. For instance, the CRAMM toolkit automates the use of the BS7799 standards (Cramm 2006). Some of the early CIIP efforts in this context includes the SimCIP (Simulation for Critical Infrastructure Protection) tool being developed within the IRRIS project (IRRIIS 2006).

enforcing laws and regulations. Most importantly, governments are expected to achieve all this whilst safeguarding the interests of its citizens. To that end, most strategists and policy makers now advocate public-private partnerships (PPP) for effective CIIP by leveraging the unique strengths of governments and the private sector. Successful PPPs for CIIP require strong accountability mechanisms that provide alignment between the incentives of the private and public sectors, as well as transparency in the sharing of CIIP-related information (e.g., security flaws, threats, etc.) among all stakeholders – even those considered as competitors (Assaf 2007). The latter requirement relies on the existence of trust and government intervention in getting the optimum balance between competition and cooperation, in order to meet agreed CIIP objectives without compromising business interests. An example PPP is the Finnish National Board of Economic Defence (NBED) that constitutes a network of committees of leading experts from both the public and private sector. The primary task of NBED is to manage, co-ordinate, and monitor preparedness in different sectors, with the information society being one of the seven designated focus sectors. Notably, NBED has the legal right to obtain information for planning and organizational tasks from actors in the private sector, this being based on the 1960 Act on the National Board of Economic Defence (238/1960).⁸⁸

Economic dimension

The implementation of CIIP measures (emergency preparedness) supplementary investment for installing redundant elements to eliminate single points of failure, robust backup power arrangements, equipment retrofits, enhanced surveillance, early warning capabilities, automated decision making tools, supplementary training for staff, thorough employee screening, and so forth.⁸⁹ However, expenditure (particularly in the private sector) is mostly driven by market forces, whereby investment decisions are dictated by the bottom line and by shareholder sentiment. This naturally tips the balance in favour of maximizing returns rather than of operational stability. Therefore, in a competitive environment CII owners would mostly invest in protection measures against frequently-occurring and anticipated threats (e.g., viruses, DDoS attacks, accidental transmission cable severance etc.) to ensure continuity of business processes. This may involve, deployment of IT security solutions (e.g., antivirus software, firewalls, intrusion detection systems etc.) and implementation of resilient network architectures to meet carrier-grade service benchmarks, such as, guaranteeing 99.999% service availability.

The overall consequence of these market pressures has been the virtual commoditization of protection, whereby information security investment decisions

⁸⁸ By contrast, the Critical Infrastructure Information Act of 2002 used by the US Department of Homeland Security (DHS) only requires information to be provided on a voluntary basis. This has meant there is a continued reluctance by the private sector to provide key information for CIP/CIIP (EIIP VIRTUAL FORUM 2006).

⁸⁹ For example, a recent study titled “The Stern Review on the Economics of Climate Change” projected that OECD countries will spend in the range of €11 – 110 billion each year (equivalent to 0.05 – 0.5% of GDP) to make infrastructure (including CII) and buildings resilient against effects of climate change (Stern 2006).

are dictated by the perceived vulnerability, threat likelihood and ensuing cost due to a realized threat (Anderson and Moore 2006)⁹⁰. The latter combines immediate costs attributed to revenue loss, asset damage, settlement costs, legal exposure, productivity losses, as well as intangible costs related to market perception and customer churn. Moreover, expenditure on protection measures also becomes correlated to the willingness of end users to accept a service surcharge for a given level of protection. This is usually expressed in service level agreements (SLAs) between the provider and the subscriber, whereby the degree of protection afforded (e.g., availability, encryption level etc.) varies according to service classification.⁹¹ Worse still, most CII owners are maintaining a prudent view on additional expenditures due to the free spending (e.g., on inflated third-generation mobile license auctions) of the 1990s that precipitated into the bursting of the dot-com bubble and the eclipse of telecom boom in early part of this decade⁹².

On the other hand, CIIP objectives specifically target high-impact events (e.g., targeted DDoS attacks on Estonia, Hurricane Gudrun in southern Sweden etc.) that result from low-probability, uncertain, unexpected or even unknown threats. Unfortunately, the true level of risk associated with such threats may be difficult to discern, making the argument for supplementary security investments for CIIP unjustifiable using traditional threat-based cost-benefit analysis and risk assessment methodologies. These methods usually prioritize security measures against high-probability known threats with a potential cause medium or high-impact disruptions. Unfortunately, by relying on hard intelligence and reactive responses to previously seen attacks, this threat-based approach leaves a large security gap exploitable by surprise attacks. Alternatively, by basing security investment decisions on the vulnerability-based approach, it is possible to ignore the threat probability in the analysis, thus clearly highlighting the potential benefits of CIIP investments (Rauscher et al 2006). Consider Figure 29, which illustrates the cost versus security level relationship under the vulnerability-based approach. The highest level of security investment justifiable for protection against known threats is reached at an optimum point that guarantees maximum returns on the investment. However, this investment is lower than that required for protection against unknown threats, thus creating a CIIP investment gap, which in turn translates into a high-risk security gap with a potential to cause great financial loss when breached (see Figure 29).

⁹⁰ See, for example, Sherwood et al. (2005).

⁹¹ See, for example, Fawaz et al. (2004). They propose a platinum, gold, silver and bronze service classification, where for instance, service recovery time is <50 ms and <5 min for platinum and bronze classes respectively.

⁹² The events followed a major sell-off of technology stocks that triggered significant drops in the technology-heavy NASDAQ index. This led to reduced spending, hiring freezes, layoffs and large inventories of unused equipment in technology companies. For detailed accounts, see reports for example (Smart Economist 2005).

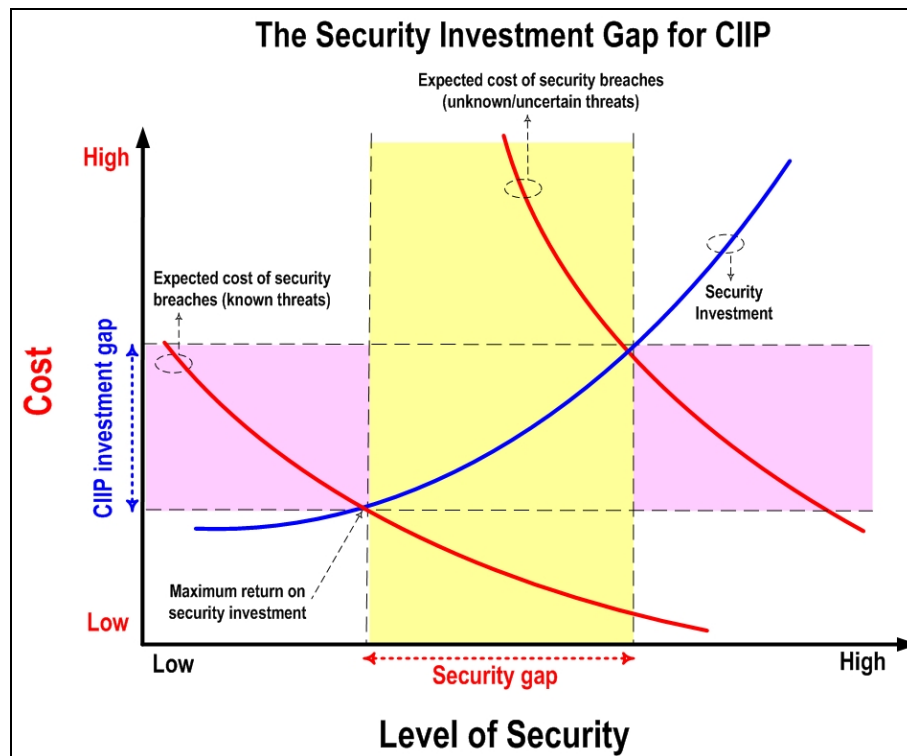


Figure III—29 Security investment gap for CIIP observed under the vulnerability based approach.

Getting an agreement by stakeholders to close the CIIP investment gap is a huge challenge. But rather than wait for market forces to drive security investment to CIIP levels, a restructuring and clear definition of persuasive arguments is needed to create the necessary willingness to take this important step. To that end, the promotion of better understanding of the interdependencies and the far reaching consequences of CII disruptions by caused high-impact events may influence investment decisions and fuel necessary efforts for the mobilization of sufficient financial resources, possibly within a PPP framework. Perhaps inspiration or lessons could be drawn from the approaches employed in other sectors. For instance, Andersson and Malm point out that many governments consider the PPPs in the energy sector as being bodies that define the government role in closing the gap between the desired and market-achievable security, but they caution on the resulting over-reliance on government bailouts (Andersson and Malm 2006). Other alternatives explored include the use of insurance not only to cover for losses incurred due to high-impact events but also induce information security investments required for CIIP (Auerswald et al 2006). Recently, the ARECI study conducted for the European Commission (EC),⁹³ surveyed over 150 key European expert CII stakeholders, and found that only 7% of the respondents thought security investment was at an acceptable level, but also 85% believed that government incentives are necessary to close the CIIP investment gap. Such trends

⁹³ The Availability and Robustness of Electronic Communications Infrastructures (ARECI) study for the EC was completed in early 2007. Comprehensive reports on its findings and recommendations see (ARECI 2007).

and opinions indicate that the economic dimension may present extremely formidable but surmountable challenges that require truly committed and decisive strategic actions.

Social dimension

The relative influence of the social dimension on the functional state of information infrastructures is arguably more pronounced compared to other infrastructure types. For instance, in utility infrastructure the commodity (e.g., electricity, water, gas etc.) is mostly delivered on a one-way path from the source or point of generation to the end users, thus limiting the way in which the end user could influence the functional state the infrastructure. By comparison, the information infrastructure affords end users bidirectional connectivity to both receive and send the primary commodity (payload or information), the ability to interact with infrastructure elements anywhere around the globe, and the increasing capability to customize their own services, profiles and so forth. Signs abound of increased confidence within these empowered users, from the proliferation of feature-rich Smartphones to the thriving Web 2.0 hosted applications and communities.⁹⁴

However, the mass adoption of ICT devices provides an increasing security challenge, as each user terminal not only presents a sitting target for threat actors but may also serve as a launching point for attacks on the networks to which they are connected. For instance, personal computers connected to the Internet could have their computing power harnessed to perform some useful computationally intensive calculations (e.g., for the design of life-saving drugs) (Buyya et al 2003). Unfortunately, cyber criminals may use similar principles to form a ‘botnet’ comprised of thousands of compromised computers or zombies that launch e-mail spam, malware, identity theft attempts and many other nefarious schemes (Goth 2007)⁹⁵. To that end, individual users should also be considered as one of the key security factors when addressing overall CIIP strategy. As some IT security experts note, humans tend to be the weakest link in the security chain (Granger 2006). This calls for an intensification of strategic actions by relevant actors in both the public and private sectors that specifically target individual users of ICTs. These actions may include:

- *Increasing Security Awareness:* Threat actors are always looking to capitalize on user ignorance, negligence and susceptibility to social engineering attempts. Awareness of the risks involved in routine actions, such as: surfing the World Wide Web with a browser’s security level set to ‘Low’; opening emails received from unknown sources; or leaving a mobile handset default PIN code of 0000 or 1234 unchanged, is a significant step in countering security threats. A user who is reasonably

⁹⁴ The latest (August 2007) figures from the web monitoring company Alexa indicate that the Web 2.0 websites such as YouTube, MySpace, Baidu, Orkut and Facebook feature prominently in the list of top 10 most popular sites (ALEXA 2007).

⁹⁵ Goth (2007) quotes an industry insider stating “Now I think of botnets as grid computing gone bad — they have infinite free computer power and free bandwidth. There is no way to stop this problem if you’re trying to do it yourself. Your costs will scale with the amount of attacks you’re receiving.”

sensitized on the security aspects of the ICT systems he/she employs, is less likely to fall prey to attack attempts. The sensitization processes may include: tips and tutorials in mainstream media and web portals, basic-level (but hands-on) courses on information security in educational/training institutions,⁹⁶ and public outreach campaigns that bring information security to the forefront of public consciousness.⁹⁷

- *Providing Support or Assistance:* The ICT proficiency of end users tends to vary widely, whereby at the high end of scale ‘tech-savvy’ users are generally able secure themselves adequately or may have the knowledge on how to respond correctly if they do succumb to an attack. Unfortunately, that class of users is very much a minority, and hence the majority of users need some sort of assistance in ensuring security and rational responses under pressured conditions. This may require a multimedia-based universally-accessible channel for providing assistance, in the same way citizens are able to promptly summon civil emergency services or access a helpline, or employs of an organization are able to call on their IT support staff. Further actions may include improved accessibility and usability of security tools, and providing guidelines on the responsible use of ICT devices, particularly in the aftermath of a crisis.⁹⁸
- *Increasing Vigilance:* Early warning capability is one of the key aspects that need to be developed sufficiently for effective CIIP. This is noted in the importance of CERTs in handling incident reports from public and private sector organizations, and usefulness in providing an up-to-date snapshot of the general security picture. Similar vigilance should be strongly encouraged from all ICT users across society and a user-friendly mechanism be made available to make reporting of security incidents simple and straightforward.

Technological dimension

Information security relies on technological advances - such as, biometric technologies (e.g., fingerprint readers, iris scans etc.) that reduce reliance on traditional authentication methods (e.g., PINs, passwords etc.) for increased robustness. However, information security is more than just an issue of technology, as illustrated by the organization model of Figure 27. To that end, the CIIP challenge involves not only coping with the fast paced ICT innovation and evolution within the techno-physical node, but also correctly anticipating the influence that these changes will exert on the other nodes within and beyond an

⁹⁶ As noted by a recent study, awareness is of no use if there is no instilled knowledge in personal security. Report by: Science and Technology Committee of the House of Lords, Britain (2007).

⁹⁷ An example campaign the National Information Security Day in Finland overseen by the governmental Information Security Committee. The campaign has included the launch of an online learning security center for schools. Following suit, an Information Security Day is now observed in Europe and beyond.

⁹⁸ For example, in the light of the mobile network congestion after the 7/7 London bombings, the operator Vodafone UK has strongly advised subscribers “to avoid making unnecessary or lengthy phone calls and, preferably, send a text message” during future crises (Fildes 2006).

organization. Evolutions in the ICT sector are now reflected by the scaling of network capacities, as well as the abundance of new and innovative concepts (e.g., fixed and mobile telephony convergence, service-oriented architectures, ubiquitous information, ambient intelligence, mobile workforce etc.) illustrated in the current migration towards Next Generation Networking (NGN)⁹⁹ and beyond. The future becomes even more unpredictable with the onset of various disruptive technologies, such as, nanotechnology and radio frequency identification (RFID).

A common theme envisioned in both the immediate and distant evolution stages is the migration from networks with centralized management, towards more flexible networks with widespread autonomous intelligence built into their individual systems.¹⁰⁰ This flexibility is made possible by the use of IP-based communications as the common denominator, allowing seamless service and application handover (transfer) between heterogeneous infrastructures, regardless of their ownership or underlying technology. To that end, significant changes are anticipated in all conceptual layers:

- *Infrastructure Layer*: The changes can be viewed from both the network and user perspectives. On the network-side, there is migration towards highly connected but survivable mesh architectures, and spontaneously organized ad-hoc wireless networking for ubiquitous connectivity shorn of centralized control and infrastructure support. On the user-side, there is the adoption of multi-standard communication devices that can be automatically reconfigured to function over multiple infrastructure types.¹⁰¹
- *Service Layer*: Migration towards context-aware services that adapt automatically and in real-time to the dynamic user context, even anticipating user needs, anytime and anywhere. The user context here refers to the users' history, personalization and preferences, terminal and network capabilities, location and mobility; organizational restrictions and procedures; and the operating environment. The process of adapting to a different context should occur without the user necessarily being aware of the technical details.
- *Application Layer*: Migration towards context-aware applications that adapt automatically and in real-time to the dynamic user context and possibly even anticipate user needs anytime and anywhere.

The incentives for aforementioned evolutions from point of view users (both individual users and those within an organization) includes, the promise of unfettered access to advanced feature-rich services and applications, increased efficiency and productivity, and flexibility in how they utilize them and select

⁹⁹ In a nutshell, NGN enables the migration from isolated vertically-integrated application-specific networks (e.g. an organization operating separate networks for telephony and data services) to single networks capable of bearing all service types (ITU 2007).

¹⁰⁰ See, for example, Tafazolli (2005).

¹⁰¹ This refers to devices that are controlled directly by humans (e.g., handsets, PDA, laptop etc.) as well as those that perform functions remotely on behalf of humans (e.g., sensors embedded in cars, furniture, buildings, clothing etc.). The dual-mode handsets that enable users to connect to both WiFi and cellular (GSM and 3G) networks are one of the early trendsetters in this regard.

providers. On the other hand, network operators can expect improved operational flexibility and efficiency that in turn minimizes operational expenditures, rapid service launches, increased customer satisfaction and immediate returns on investments.

However, the technological advances accompanying these evolutions also increase the number of ways and instances that an information infrastructure could be rendered vulnerable. Each one of the added vulnerabilities creates opportunities for attacks from an infinite number of threats, both known and previously unknown. For example, the widespread adoption of smartphones and PDAs with local Bluetooth and Internet connectivity has introduced malwares into the mobile communications arena, a threat previously synonymous with computer networks (Hyponnen 2006).¹⁰² The security challenges are considerable as the interconnectivity and proliferation of devices goes beyond unprecedented levels, with each device and connection representing a possible security gap. Awareness of these security challenges is on the rise and some significant research is already being carried out to address them.¹⁰³

As CII becomes increasingly complex, failure prevention can never be total. Therefore, fault tolerance presents arguably the most effective method for automatic recovery from failures and their potentially highly disruptive outcomes (Liotine 2003). Fault tolerant systems are typically designed to detect failures instantly, avoid single point failures, isolate elements with persistent problems and enable repairs to be carried out even whilst continuing normal system operations. It therefore enables network user transactions to continue without any noticeable loss or interruption. These design objectives are met by providing redundancy, continuous status monitoring of network elements and automated recovery mechanisms. The majority of threat scenarios generated for CIIP studies and planning evoke scenes of destroyed or disabled infrastructure, thus necessitating methods such as fault tolerance to be designed into the infrastructure (that is, critical infrastructure protection).

However, the increased decoupling of services and applications from the underlying infrastructure in future networks creates a new inter-infrastructure dimension for fault tolerance design, whereby a service or application could be continuously available by migrating from a damaged infrastructure to a working one as a way of adapting to a new user context. An example solution is the proposed Secured Infrastructure Router (SIR) that has multiple interfaces for connecting to alternative networks as a form of redundancy against failure to any of the networks (Kari 2007). Such capabilities present a paradigm shift to critical information protection within the CIIP concept, as it shifts the emphasis to availability, confidentiality and integrity of user's information over a particular service or application, from traditional infrastructure protection. This service or application level protection mechanisms present significant cost and time advantages in comparison to preventing attacks by fortifying every node,

¹⁰² The number of known mobile malware nonexistent before 2004 has risen sharply to over 200 in late 2006. This is small when compared to over 200,000 known computer malware. However, with the number of mobile devices connected to Internet expected to significantly outstrip the number of PCs, the threat of mobile malware is likely to be a formidable one.

¹⁰³ See, for example, Calin et al. (2006).

telehousing facility, cell site and length of cable of a network infrastructure. Moreover, it further emphasizes the need for cooperation between different CII owners to enable recovery of key services and applications (e.g., 112 emergency services) between their respective infrastructures, especially in moments of crises.

3.4 CONCLUSIONS AND WAY FORWARD

National

Most of the countries in the BSR are widely acknowledged as current models of leading information societies. Accompanying this success are the multiple challenges of CIIP to ensure delivery of key services and supplies, economic stability, and maintenance of overall national security. Governments are now addressing these challenges in various policy statements and strategic plans. For instance, the Finnish government recently issued a Government Resolution on The Strategy for Securing the Functions Vital to Society, whereby the importance of a the information and communications systems is stressed in almost all of the society's vital functions. Most importantly, the government places particular emphasis on the need for interagency cooperation as a means for securing vital functions (SSFVS 2006; see also Kaskeala 2006). A common network infrastructure - such as the VIRVE TETRA network serving multiple government agencies - is one practical example of the advocated interagency cooperation.

However, a majority of critical information assets in market economies are under the ownership of private sector organizations, a trend mirrored across the BSR. Furthermore, the interdependencies between organizations are getting increasingly complex, an attribute that renders itself to CIIP. This complexity highlights the fact that CIIP is not a problem confined to CII owners, hence accentuating the need for PPP frameworks. A PPP brings together all the national communities (public and private) with a potential stake in the CIIP efforts of early warning, detection, response, and crisis management. To that end, an effective PPP can prove beneficial to all partners, as it allows the sharing of the weight of responsibilities (including the investment in security), brings economies of scale and productive synergies are achieved. Furthermore, the cooperation between public and private partners creates a more streamlined decision making process on key CIIP projects. Moreover, cooperation provides the required analytical capacity and technical competence to understand the scope of the CIIP challenge and keep up with the effects of rapid ICT advances.¹⁰⁴

Regional

The cross-border interdependencies between organizations in the BSR are increasingly tight, particularly from the perspective of information infrastructure. For instance, NORDUnet has recently completed a fibre-based backbone

¹⁰⁴ An example effort in this regard in Finland's National Information Security Board (NISAB) composed of leading experts from the ICT and key government officials (Ministry of Transport and Communications 2004).

infrastructure that links research and higher education institutions across several countries in the region. Similarly, multinational firms in the ICT sector, such as the telecom operator TeliaSonera AB, now own infrastructure and/or have operations that span several BSR countries. These developments accelerate the need for matching regional CIIP efforts that also serve to complement the CIIP strategies being planned or implemented at a national level. The regional CIIP efforts could be based on the recognition of the commonality of risks (vulnerabilities, threats and assets) and the potential escalation or cascading of regional disruptions within the BSR - the cyber-crime incidents targeting customers of Nordea bank across the region, being one of many existing examples. Furthermore, regional efforts could be built on the potential of the extra value accrued by having robust regional CII, which translates into improved regional security, trade opportunities and other economic spill-overs. Examples of some of the early regional CIIP efforts in the BSR include:

- Example 1: The conception of cross-border TETRA-based PSS networks as part of the general effort to improve cooperation between government agencies operating in local regions either side of national borders. The initiatives with the BSR includes: the existing sharing arrangement between the Finnish VIRVE network and Estonian authorities (Laanet 2007), the envisioned interconnection of the Swedish (RAKEL) and Norwegian (Nodnett) PSS networks (Vollan 2006), as well as exploratory talks between Polish and Lithuanian officials for future PSS interconnection (Police Ministry of Interior 2007). Coincidentally, the vision of such cross-border is compatible with the Schengen treaty requirement for *“the timely transmission of information for the purposes of cross-border surveillance and hot pursuit.”*¹⁰⁵
- Example 2: The inception of a Nordisk CERT Forum (NCF) for cooperation and exchange of information on security incidents among eight academic and national CERT teams from Denmark, Finland, Norway and Sweden.

These example initiatives, while still admittedly piecemeal by focusing on only a subset of BSR countries, serve as a useful starting point for further BSR-wide initiatives (e.g., a Baltic Sea Region CERT). To that end, some form of regional or cross-border PPP with firm CIIP objectives is necessary to promote, implement and oversee the various regional CIIP strategic actions. This PPP could probably be initiated from a BSR project, such as, the BSR InnoNet project.¹⁰⁶

International

The connectivity of information infrastructure has a global reach. Therefore, the threat actors are equally global in their presence and their attacks just as effective, regardless of location. Moreover, as globalization continues to take hold, the

¹⁰⁵ Article 44 of Schengen *acquis* as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999 (European Council 1999). Majority of BSR countries are now signatories of the Schengen Agreement.

¹⁰⁶ The BSR InnoNet project is linking policymakers, agencies and analysts to create a joint innovation framework for the region (BSR Innonet 2007).

effects of a European or even global crisis now yields an even greater influence on the policies and decision-making processes of individual BSR countries. These realities combine to make the challenge of CIIP a truly international one, requiring international initiatives and programs that complement those at the regional and national levels. The EC has prioritized network and information security as one of the main hurdles that needs to be overcome on the road towards the creation of a single European information space (Commission 2006c). Furthermore, the EC launched a co-ordination project CI2RCO (Critical Information Infrastructure Research Co-ordination) that seeks to foster Europe-wide cooperation via common CIIP research platform and eliminate duplication of efforts in existing or planned R&D initiatives.

Beyond the EC, the G8 was one of earliest international groupings to address the CIIP challenge, when in March 2003 a group of G8 Ministers of Justice and Interior adopted a set of eleven principles to be considered in developing national strategy for reducing risk to CII. International associations and standardization bodies are also responding to the CIIP challenge. Notably, the ITU recently commissioned a study on generic national frameworks for CIIP to assist countries that have either been late or lack the capacity to initiate national CIIP programs (Suter 2007). To that end, the BSR countries will be expected to play an increasingly significant role on matters of CIIP and information security in general. For instance, the North Atlantic Treaty Organization (NATO) has endorsed plans by Estonia to set up a Cooperative Cyber Defence Centre of Excellence (CCD COE) that will concentrate on the needs of NATO member states (IET 2007). What is clear from all this is that CIIP challenges will be effectively tackled only by web of partnerships that are weaved initially from the national level, and eventually spread out to the regional and international levels.

CHAPTER IV: OIL TRANSPORTATION AND MARITIME SAFETY

Piia Nikula
and
Veli-Pekka Tynkkynen

Aleksanteri Institute, University of Helsinki

&

Nordregio

Nordic Centre for Spatial Development

4 RISKS IN OIL TRANSPORTATION IN THE GULF OF FINLAND. “NOT A QUESTION OF IF – BUT WHEN”

4.1 INTRODUCTION

The Baltic Sea is one of the most important passages for trade and tourism between the Nordic and Baltic countries. It has gained in importance due to the enlargement of the European Union and to the boost to Russia's economic development. Oil transportation from Russia has increased drastically with the opening of the new Russian oil terminals.

The Gulf of Finland, in addition to the Danish Straits, forms the narrowest and shallowest waters in the Baltic Sea. It is one of the most heavily trafficked sea areas in the world. According to HELCOM (2006a), the Helsinki Commission – Baltic Marine Environment Protection Commission, over 2,000 passengers or cargo ships sail the Baltic at any time. This increases the area's risk level.

This case study examines the situation of the increasing oil transportation in the Gulf of Finland, and the present sea transport safety solutions for the region. By studying what is being done, the aim is to identify the possible safety gaps in the maritime transportation and consequently make recommendations on how to improve the safety situations in the form of actual policy proposals.

Methodology and previous research

This study combines quantitative and qualitative approach. The data used in the maps and illustrations is gathered from existing research reports, whereas the qualitative input has been gathered from interviews with experts in Estonia, Finland and Russia. In the interviews, the main point has been to ask the experts to discuss and evaluate the level of risk, to consider the importance of recommendations and guidelines already made, and to reflect on whether they see their role as being sufficient and what they consider to be lacking in the safety and security measures.

There are many studies on the state of the Baltic Sea. The majority of them emphasize the environmental protection, especially those made by HELCOM, but there are plenty of research (reports, recommendations, analyses) into the risks and threats related to maritime traffic. This study is less academic and more policy-oriented. Many studies include recommendations and policy guidelines for the Baltic Sea States to use. Some examples include VTT Technical Research Centre of Finland (e.g., Rytkönen 2006 and 2007, Rytkönen and Semanov Gennady 2005, Meriturvallisuusseminaari 2007, Cleaner Seas 2007), and Baltic Master.¹⁰⁷ The

¹⁰⁷ Baltic Master is a EU Interreg BSR IIIB part-financed international project that aims to improve maritime safety by integrating local and regional perspectives. The focus is on the Baltic

Finnish WWF released recommendations in 2007 regarding maritime safety and the close calls that took place on the Gulf of Finland during winter 2007 (WWF Finland 2007a). At the Karlskrona workshop held in Sweden (Räddningsverket 2001), one of the conclusions was the identification of the need to connect all the Baltic Sea States' rescue services in order to fulfil the main objective of increased understanding and the effective use of common resources in oil spill prevention.

Premises for studying oil transportation in the Gulf of Finland

The subtitle of this study tells much about current thinking concerning the situation in the Gulf of Finland. There has not yet been a large-scale accident, but if an oil accident should take place in the Gulf of Finland, it would be catastrophic, especially to areas with extensive archipelagos. Collecting oil in a fragmented archipelago is far harder than from a continuous shore line. All this is well known, and it is usual for human nature to live with a certain level of risk.

However, this outlook might be changing. Comprehensive approaches to maritime safety issues are called for by many forums and they include issues such as risk assessment, preparedness and prevention plans, alarm and warning systems, investigation of accidents and environmental crime and planning of response operations, including for oil spills.

The emphasis is therefore on prevention and on efforts to stop accidents from happening. The oil transports are part of, and consequently maintain, the critical infrastructure in their destination areas. Their securing is vital, and has been included in the EU agenda in the protection of the European Critical Infrastructures (ECI) and National Critical Infrastructures (NCI). Passenger traffic is also included in rulings on the protection of people's movements. It is therefore essential to look at these two dimensions of traffic together when evaluating the safety situation in the Gulf of Finland. However, because maritime security is to be enhanced relating to the European Programme for Critical Infrastructure Protection (EPCIP) and its goals, it is important to bear in mind that protective security measures should not be more intrusive than are strictly necessary.

4.2 OIL TRANSPORTATION IN THE GULF OF FINLAND

Description of the area

The Gulf of Finland forms the 400 km long easternmost part of the world's largest area of brackish water, the Baltic Sea. The shores of the Gulf are occupied by a fine grain archipelago, especially on the Finnish side of the Gulf. There is also an extensive archipelago in Russia's national waters, adjacent to the Karelian Isthmus. Estonia's shores do not have an archipelago, which is the consequence of sand and limestone bedrock found in the area. However, in the westernmost part of Gulf of Finland there are two large islands, Saaremaa and Hiiumaa, belonging to Estonia. The Northern shores of the Gulf of Finland are formed of granite and

Sea Region and issues concerning preparedness, prevention and marine spatial planning. See <http://balticmaster.org>

other old bedrock minerals, making the area rich in smaller islands. Fact Box 1 and Figure 1 indicate how shallow the Gulf is in the Eastern and Northern archipelago.

Gulf of Finland

Physical dimensions:

- Approximate length 400 km
- Width 60-135 km
- Maximum depth 60 m
- Average depth 37m (Neva Bay only 5-10 m)

Environmental indicators:

- Brackish water, salinity ranging from 0,4 ‰ in the Neva Bay to 1,1 ‰ in the Western part of the Gulf of Finland (in the Atlantic Ocean 3,5 ‰)
- Bottom layers of water are oxygen free (lifeless layer) and surface waters occupied yearly by algae blooms due to excessive nutrient load
- Partly ice-covered from December till April

Fact Box IV—1 The Gulf of Finland. (Merentutkimuslaitos 2006 and Sonninen et al. 2006, pp. 14-16.)

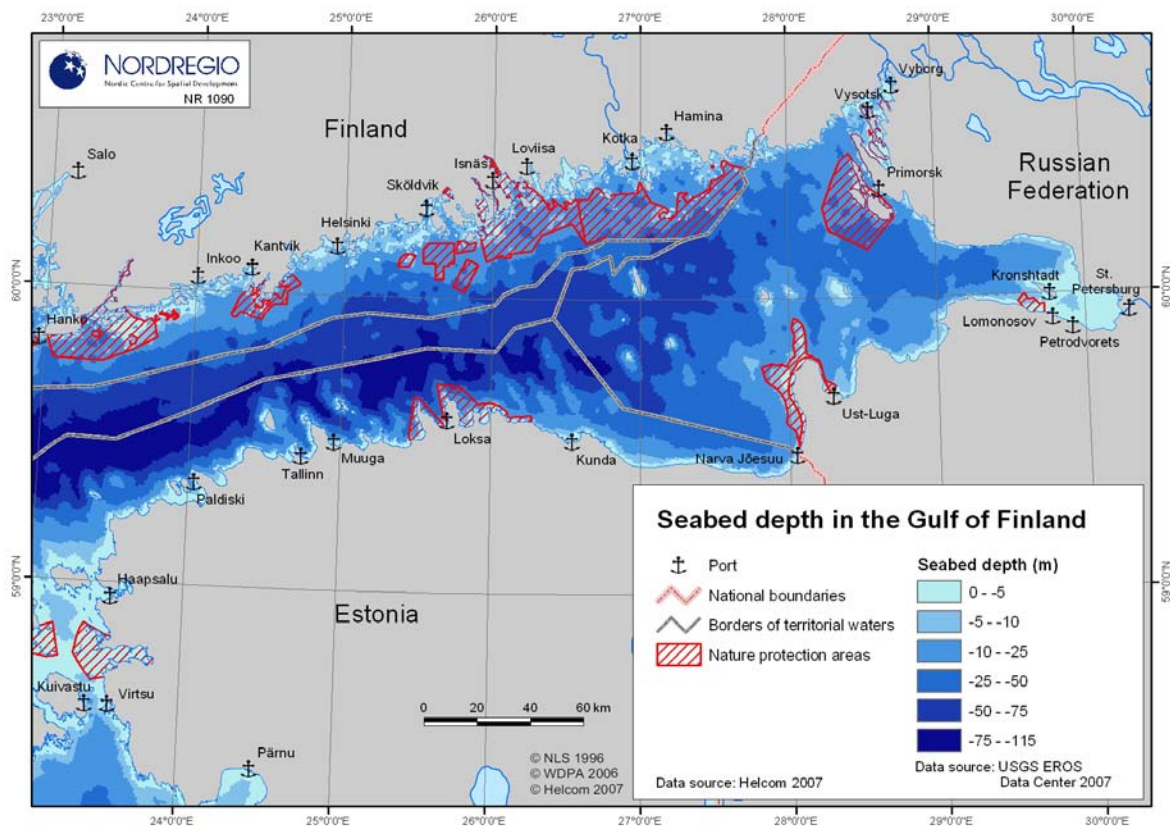


Figure IV—1 Seabed depth in the Gulf of Finland.

Oil tanker traffic among cargo and passenger ships

The EU's external dependence on energy is increasing and the Russian oil transported by sea plays ever more important role. Europe represents about a third of the global market for crude oil. Ninety percent of that oil and refined products are transported by sea to and from Europe. The volume of oil transport is especially heavy in the Gulf of Finland, because Russia is building more port infrastructure here.

Many estimates say that the overall traffic and transportation of potentially hazardous cargo, especially oil, have more than doubled since the late 1990s. This has increased the volume of traffic and has made the traffic routes increasingly congested, especially during winter. Furthermore, the role of the Gulf of Finland has increased, because Russia wants to transport oil through its own ports, thus diminishing the importance of the Baltic States as oil transit countries. The increase in the volume of transported oil will most probably also be the trend in the future (Ministry of Transport and Communications in Finland 2005), as shown in the figure below.

There are several oil ports on the shores of the Gulf of Finland, including Muuga, Primorsk, Porvoo, Naantali and St Petersburg, which are among the biggest on the Baltic Sea (HELCOM 2006b). The turnover of Muuga, Primorsk, Porvoo and St Petersburg oil terminals has grown by over 250% since 2000, and over 400% since 1997 (HELCOM 2005). Primorsk has experienced the largest growth due to the fact that its oil terminal, connected to the Baltic Pipeline System (BPS), was opened only late 2001 (Figure 2). Figure 3 shows the amounts of overall traffic, i.e. vessels of all types entering and leaving the largest ports of the Gulf of Finland. It describes well the equation of growing cargo traffic combined with the heavy passenger traffic and oil transportation forming the smallest part.

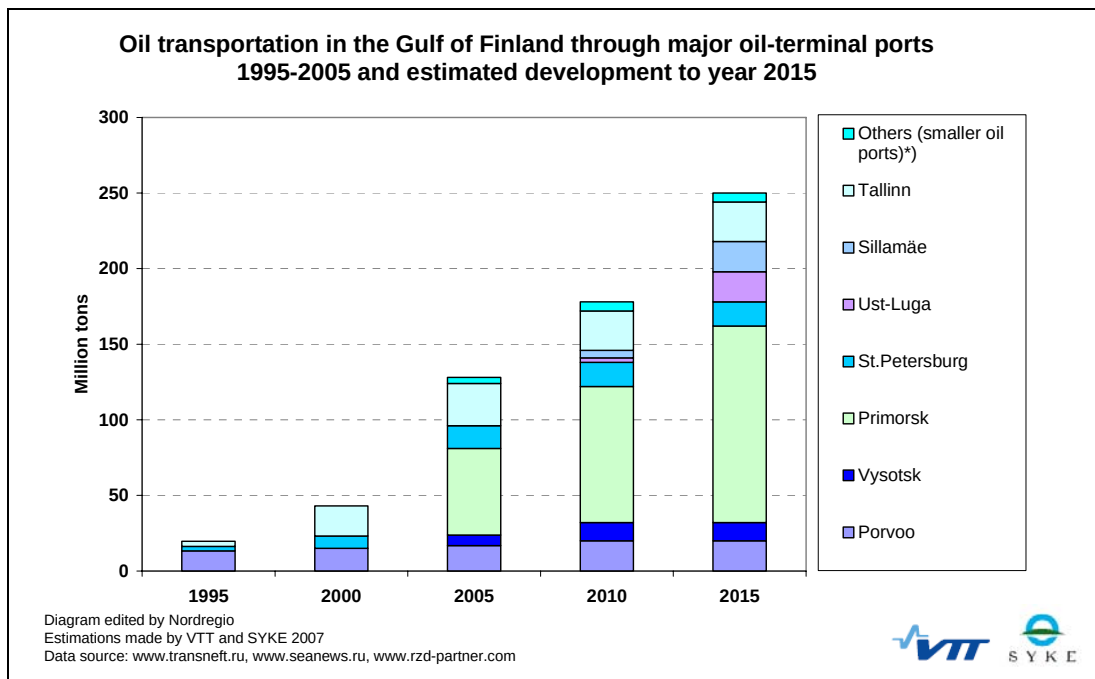


Figure IV—2 Oil transportation in the Gulf of Finland through major oil-terminal ports 1995-2005 and estimated development to year 2015. (SYKE and VTT)

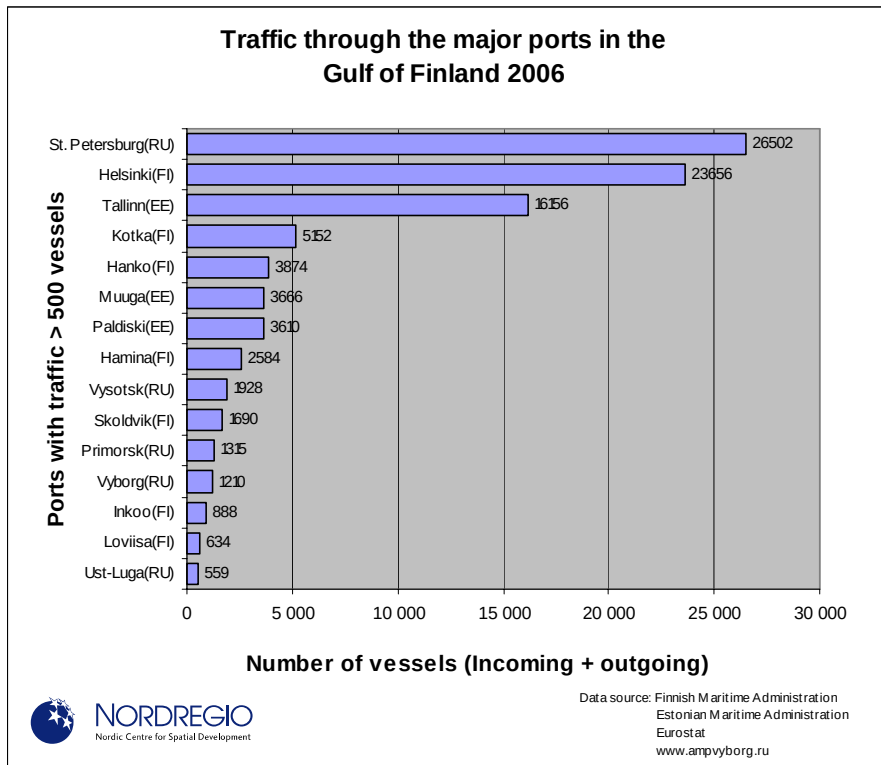


Figure IV—3 Traffic through the major ports in the Gulf of Finland 2006.

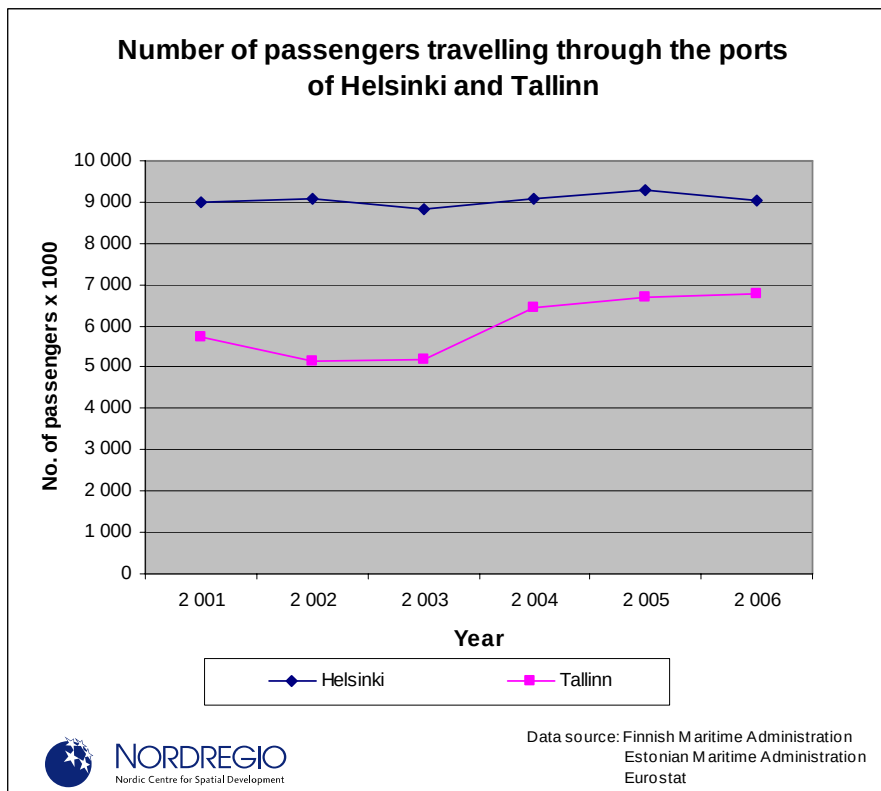


Figure IV—4 Number of passengers travelling through the ports of Helsinki and Tallinn.

In addition to the increasing oil and cargo transportation traffic, the Gulf of Finland is burdened by heavy passenger traffic, especially between Helsinki, Finland, and Tallinn, Estonia (Figure 4). In 2005, this traffic comprised 40,000 vessels (HELCOM 2006b), including both passenger and freight transport. The criss-crossing traffic of oil transports and passenger traffic in the Gulf of Finland constitutes a big challenge for the surrounding countries, both in the western part of the Gulf of Finland, with traffic lanes from Finland, Estonia and Russia (Figure 5), and in the eastern part closer to Russia where traffic from St. Petersburg / Primorsk and Vyborg / Vysotsk exits and enters the main traffic lane of the gulf (Figure 6).

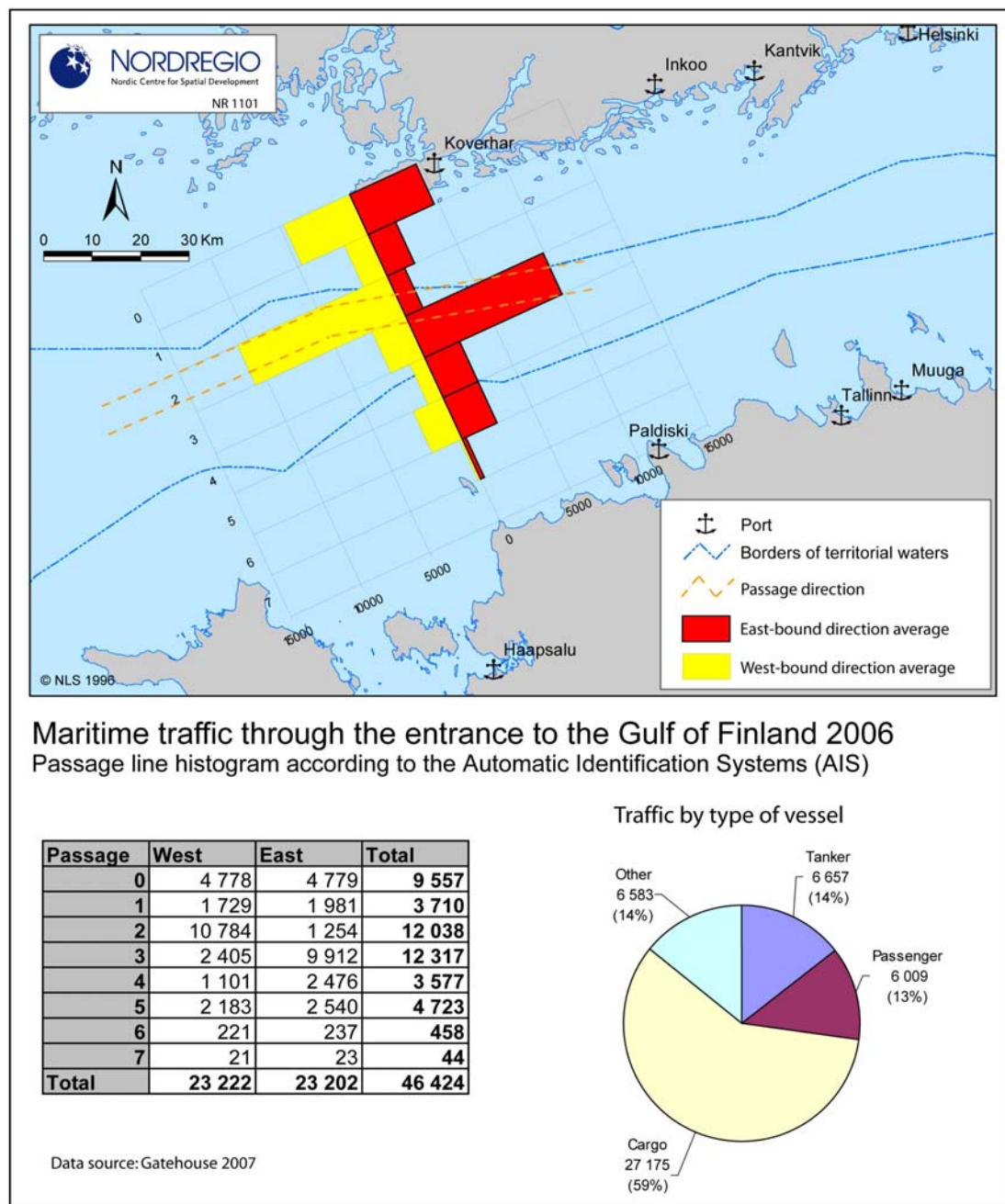


Figure IV—5 Maritime traffic through the entrance to the Gulf of Finland 2006.

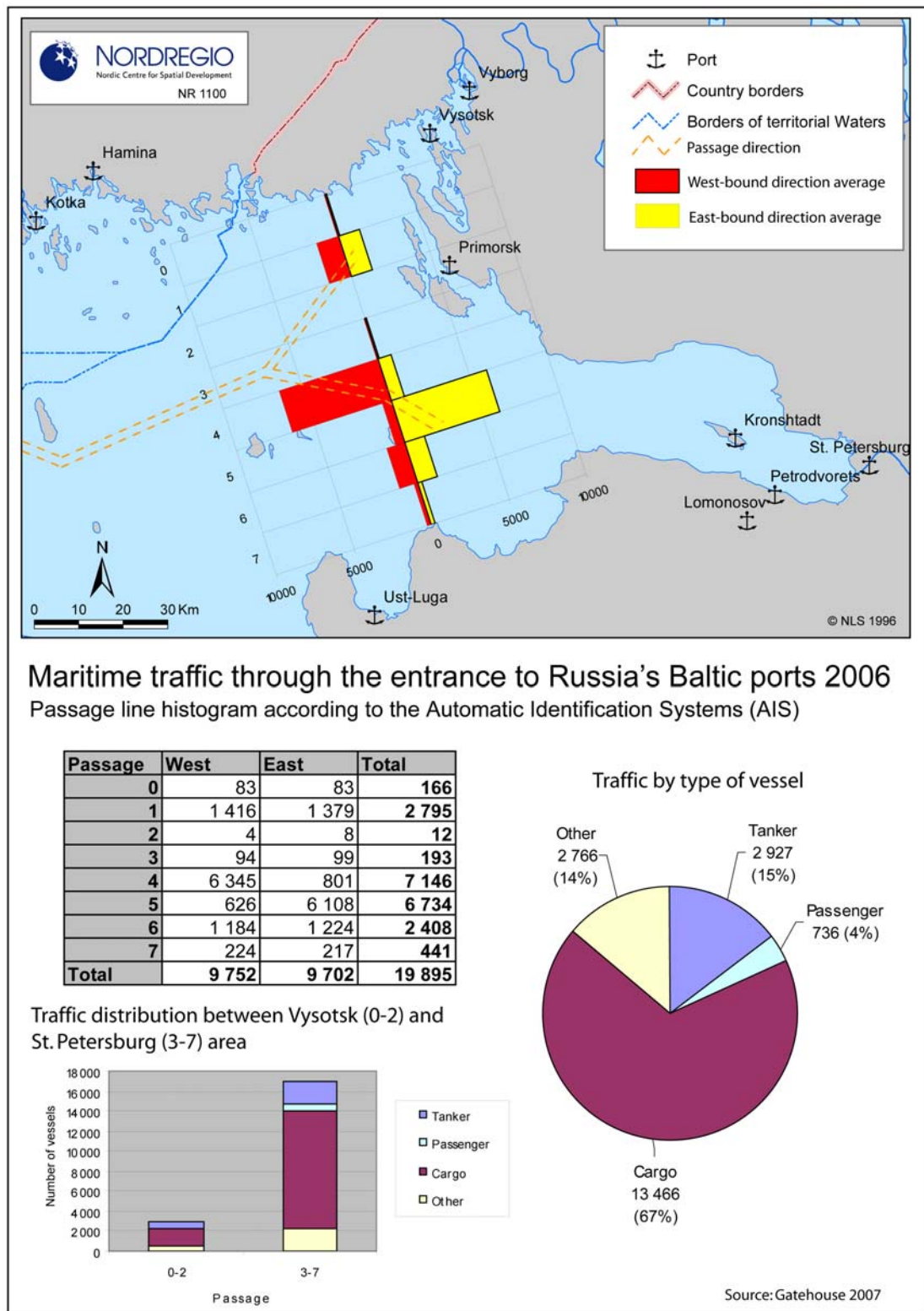


Figure IV—6 Maritime traffic through the entrance to Russia's Baltic ports 2006.

4.3 RISK EVALUATION

Risk perceptions of the Finnish, Estonian and Russian maritime authorities

Close-calls and accidents in maritime transport are not new phenomena in the Gulf of Finland. This is due to the challenging geographical conditions of the sea, difficult weather conditions in the winter time and increasing traffic. However, the Baltic Sea Region (BSR) and especially the Gulf of Finland can be determined as a fairly low risk area from safety (accidents) and security (terrorism) viewpoints, so far with only minor-scale incidents. There have e.g. never been any terrorist strikes in the area (during the time of the modern states of Estonia, Finland and Russia), neither have there been large oil accidents. The biggest catastrophe in the Baltic Sea happened in the 1994 when the passenger ferry MV Estonia sunk near the Finnish coast due to a technical failure. Despite the still ongoing discussion about the possibility of terrorist-related cause in the sinking of ship, it is the consensus in the area, expressed in the evaluations made by Maritime Authorities (MA) of the respective countries, that guaranteeing the safety enhancing procedures of vessel traffic in the Gulf of Finland is far more important than security-related procedures.

This study uses published material as a background against which the risk perceptions of the interviewed marine specialists, representing the MA and related institutions of Finland, Estonia and Russia respectively¹⁰⁸, are compared. Identification of risks, or what is at risk, is always contextually and culturally specific. In this case, despite culturally and politically representing different contexts, interviewees all belong to the same professional reference group. Each of them has a maritime background in terms of education and practical work, subsequently accompanied by experiences in marine traffic control. The following sections will elucidate the safety risks that rise from the views of marine authorities when they were asked about the risks.

We have tried to analyse this qualitative data bearing in mind that the conceptions of the interviewees should not be taken as fact, but as personal, though professional, views about the vessel traffic safety (and security) situation in the Gulf. Naturally, these views are formed and moulded by the personal and professional histories of the interviewed MA.

The risks in the Baltic Sea can be described as cross-border ones. One definition describes a cross-border risk as a potential civic and systemic risk that

¹⁰⁸ The authors are most thankful to the following people who kindly agreed to be interviewed for this study: Matti Aaltonen, Director, Vessel traffic management, Finnish Maritime Authority, 6.6.2007 in Helsinki; Kari Kosonen, Vice director, Vessel traffic management, Finnish Maritime Authority, 6.6.2007 in Helsinki, and 25.9.2007 by telephone; Rein Haavel, VTS Project Office Manager, Cybernetica Ltd., 7.6.2007 in Tallinn; Are Piel, Head of Vessel Traffic Services Department, Estonian Maritime Authority, 7.6.2007 in Tallinn; René Sirol, Deputy Director General, Head of Maritime Safety Division, Estonian Maritime Authority, 7.6.2007 in Tallinn; Ivan Gotovchits, Head of Regional Vessel Traffic Service, Ministry of Transport of the Russian Federation, State Enterprise "ROSMORPORT", St. Petersburg's branch, (answers to an e-mail questionnaire received) 31.8.2007; Vladimir Vasilyev, Deputy Director/Associate Professor, Safety of Navigation and Radio Communication, Central Marine Research and Design Institute, (answers to an e-mail questionnaire received) 22.8.2007.

affects more than one country by creating potential or actual losses across governmental borders (Hellenberg and Hedin 2006, p. 8).

Excessive environmental risks

The narrow and shallow geographical conditions of the Gulf of Finland sea area make it a high-level risk zone. The traffic volume is high its central parts, in international water, where the lanes of ‘the motorway of the seas’ are located. Despite the heavy use of the sea as a transport route, the Gulf of Finland is not seen solely as a traffic route, but as an area of important cultural heritage and environmental value.

The Baltic Sea is environmentally vulnerable and has been identified as the Particularly Sensitive Sea Area (PSSA) by International Maritime Organization (IMO) in 2005: “A Particularly Sensitive Sea Area (PSSA) is an area that needs special protection through action by IMO because of its significance for recognized ecological or socio-economic or scientific reasons and which may be vulnerable to damage by international maritime activities.” This means for example, that the estimation for the renewal of the water of the Baltic Sea is approximately 25-20 years, which causes pollutants to remain in the water for a long time.

Even if there is common understanding that on a daily basis most of the pollution in the Baltic Sea is derived from the surrounding land areas, a routine ship operation inflicts pollution too. For example, WWF Finland released a study according to which at present only 13 out of the 50 shipping companies are committed to proper treatment of sewage (WWF Finland 2007b). All the states at the Baltic Sea area are included except the Russian Federation.

Despite the shared will of all the Baltic Sea States to protect the Baltic Sea, there are differences in how the countries’ representatives perceive and value the state of the environment of the Baltic Sea, and why its protection is considered important. Estonia’s worries about an oil accident are understandable, because Estonia currently lacks equipment to collect spilt oil from the sea. Then again, the country to suffer most from an oil accident would probably be Finland, since the prevailing winds and sea currents in the Gulf of Finland area would divert oil pollution to the Finnish archipelago and the long Finnish coastline. In addition, despite what magnitudes of oil pollution combating equipment a country or region possesses, the consequences of a 100,000 ton oil tanker accident, if all of the oil were to be released, would be devastating for the whole Gulf of Finland and the Baltic Sea in general. At least one aspect of the Russian view comes from the fact that even if it has signed, it has not ratified e.g. the convention regarding the environmental protection of the Baltic Sea, the so-called “Espoo Convention on Environmental Impact Assessment in a Transboundary Context” from 1991 (EC EIA 1991).

A specific high-level risk: Wintertime ice conditions

Oil transportation has to be guaranteed all the year round and their importance is highlighted in winter, when weather conditions are at their most challenging. The Gulf of Finland freezes each year, which demands a special design and construction of the vessels intended to sail in the Baltic all the year round.. Tanker traffic is faced with the challenges caused by the ice thickness, as well as the

pressure from the ice ridges, and especially when manoeuvring in convoys led by icebreakers (Liukkonen 2006).

Even if the Baltic Sea has open water for the most of the year, the easternmost end of the Gulf of Finland is encumbered by ice for almost as long as the Gulf of Bothnia between Finland and Sweden, making it 5-6 months during a year. The ice conditions in the Gulf of Finland are exceptionally difficult. It is noteworthy that during four consequent winters in the new millennium the Gulf of Finland has frozen entirely. The easternmost end of the Gulf of Finland is also the place where the most important Russian oil terminals are situated. (Figure 7)

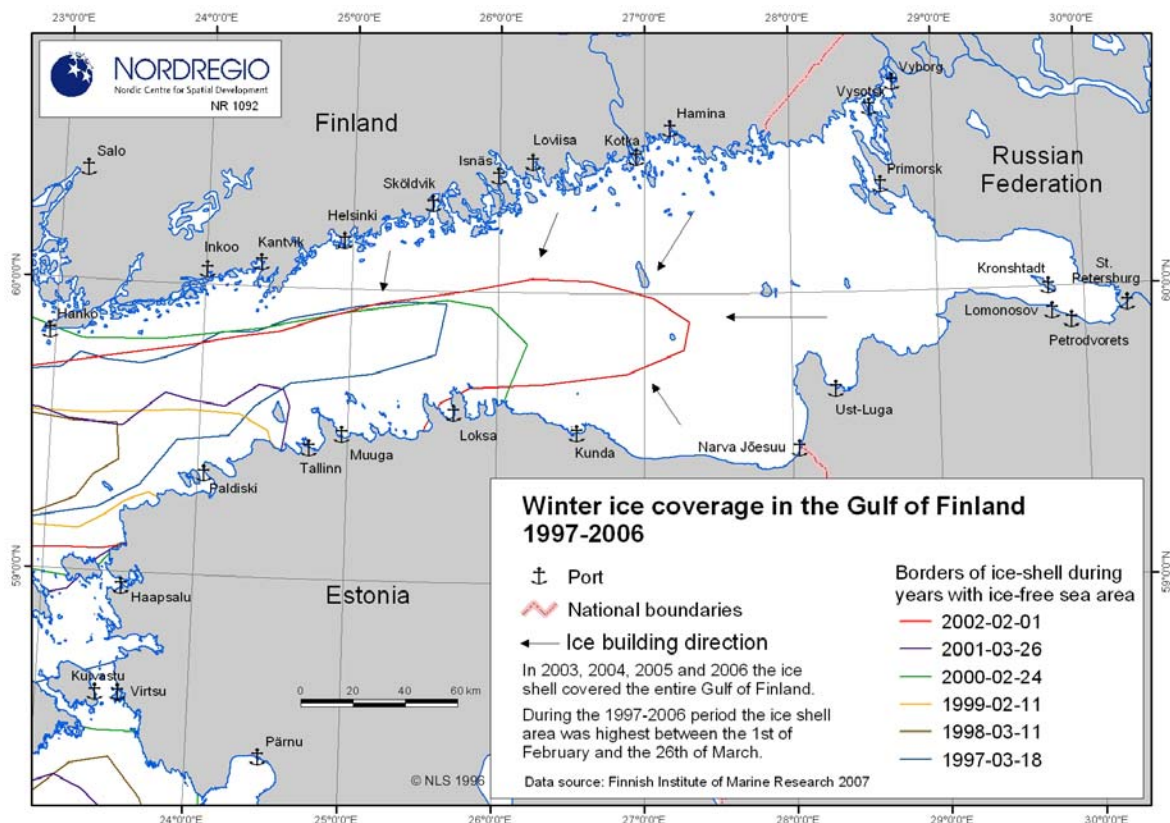


Figure IV—7 Winter ice coverage in the Gulf of Finland 1997-2006.

Because winter navigation, especially, is a growing challenge for the safety of oil transportation, it is no surprise that most of the interviewees emphasized the need for training in winter navigation. The severity of the climate and the extreme weather conditions make the Gulf of Finland among the most risk prone sea areas in the world. Navigating in ice conditions naturally causes special risky traffic situations, especially when ships are sailing in convoys led by an ice breaker. In 2005 rear-end collision led to the sinking of one of the ships in a convoy when a Russian icebreaker was halted by pack ice.

Human error and technical failures

Accidents are most often of unintentional nature and caused by human error or technical failures. According to HELCOM (2006b), the main factors leading to accidents in 2004 were human factors (39%) and technical failures (20%). These

figures were backed by the perceptions of both Estonian and Finnish MA, since they accentuated the importance of human factor as the main cause for accidents. Representatives of the Russian MA did not explicitly mention human factors as the main cause for accidents, but emphasised the central role of ships crews, especially in guaranteeing safe winter navigation.

The number of collisions has not decreased despite the many efforts to prevent them. HELCOM's statistics show that collisions have increased in relation to ships running aground, which used to be the most common type of accident. (Figure 8) These accidents involved cargo vessels (60% of all accidents), tankers (15%) and passenger ferries (12%).

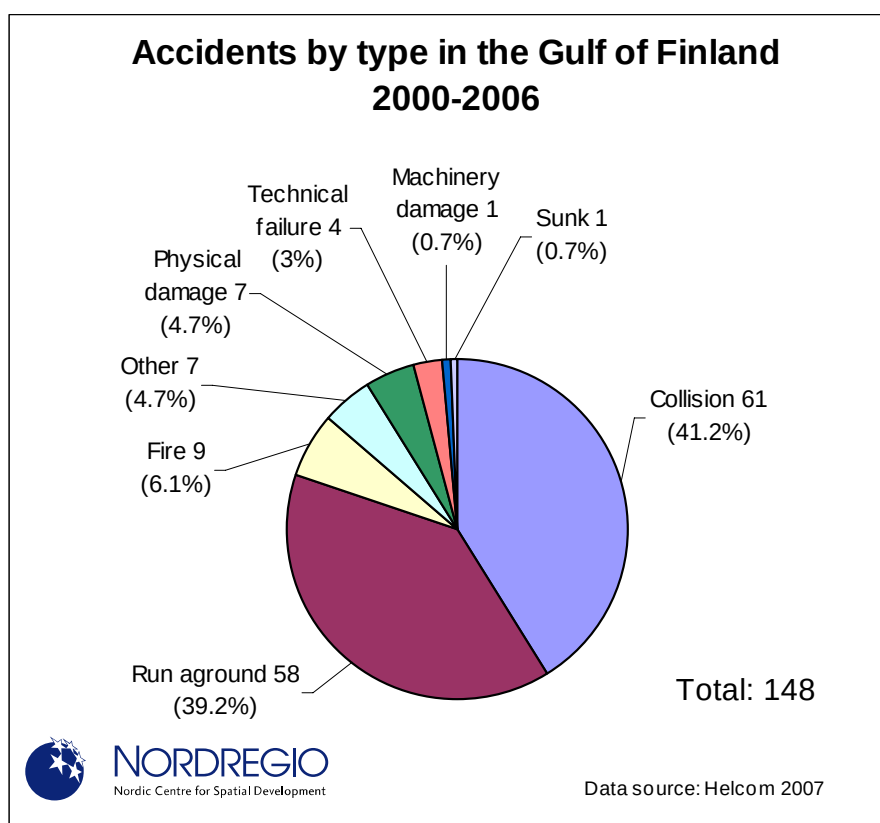


Figure IV—8 Accidents by type in the Gulf of Finland 2000-2006. (HELCOM 2007)

Growing criss-crossing traffic

According to the MA of Estonia, Finland and Russia the rapidly growing oil tanker traffic causes one of the main risks in the traffic in the Gulf of Finland. The Gulf of Finland's risk level has risen at the same rate as the traffic volume. Both the number and size of oil tankers have been growing steadily in the recent years. According to HELCOM (2006a), by 2015 an increase of 40 % is expected in the volume of oil shipped yearly on the Baltic Sea. Other estimates are even greater, and they are related e.g. to the fate of 'Druzhba' oil pipeline that runs through Byelorussia to Central and Western Europe. If it is closed, as has been mooted in Russia, the volume of oil transports in the Gulf of Finland will rise to a new level. Currently, the figure is around 150 million tonnes of oil per year.

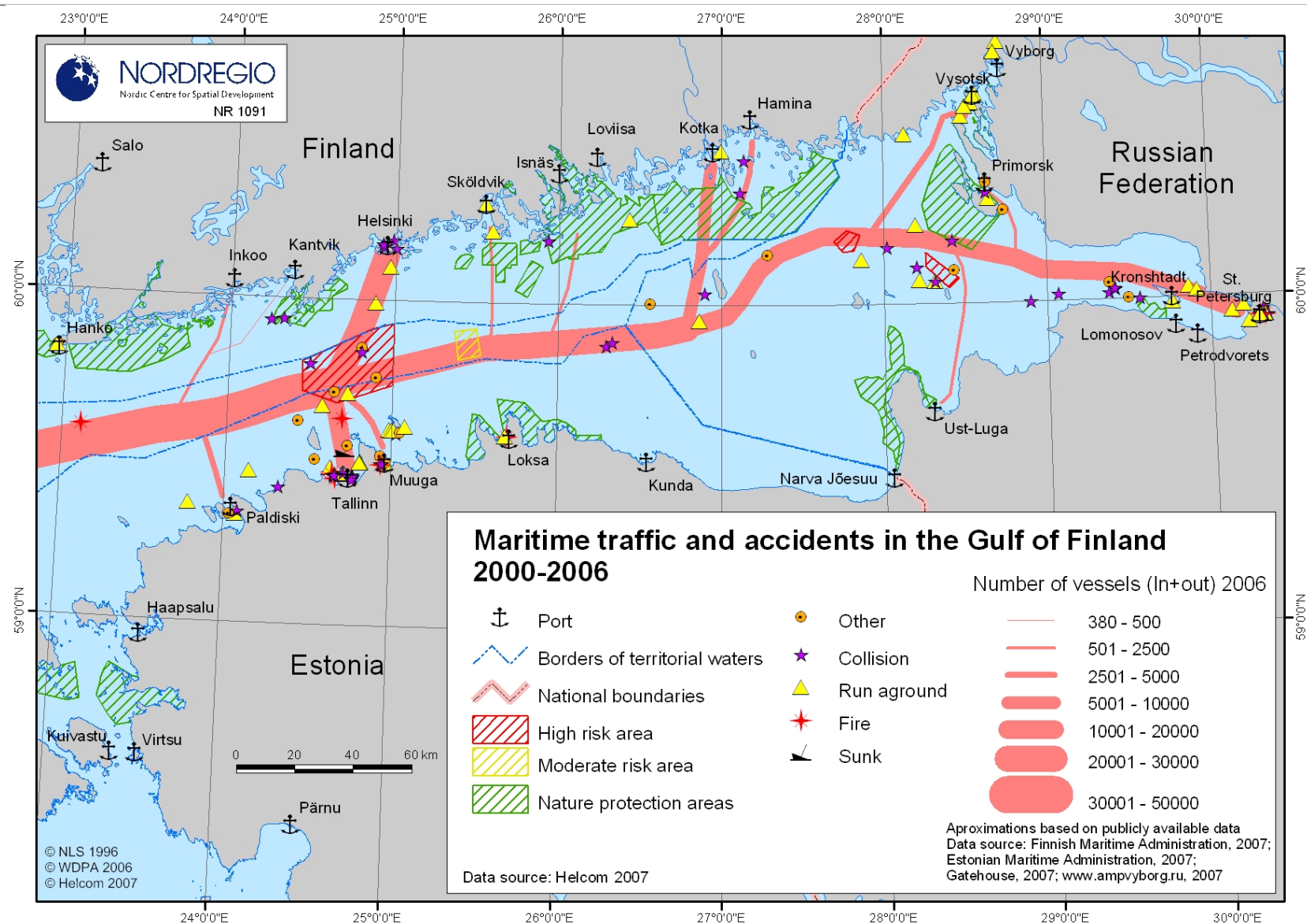


Figure IV—9 Maritime traffic and accidents in the Gulf of Finland 2000-2006.

In addition, the use of bigger tankers carrying 100,000-150,000 tonnes of oil, is expected to rise, according to Semjon Vainshtok, the head of the Russian state-owned oil pipeline monopoly Transneft (HS 2007e). The consequence is a lower risk probability due to the reduction in the amount of tankers, but with the higher risk of a large-scale accident, because of the vast amount of oil transported by one vessel. Naturally, this is true only during a certain, limited time-span, before the volume of oil transported in the Gulf will be of the magnitude that even the number of larger 100 000 tonne tankers will surpass the present number of tankers travelling in the Gulf.

All MAs shared the view that the combination of growing oil tanker traffic in the Gulf of Finland and the crossing fast passenger traffic between Helsinki and Tallinn cause a very high risk (Figure 9). However, the Estonian MA did not consider passenger traffic as the *main* cause of the risks in maritime transport. This is understandable, taking into account the importance of the passenger traffic for Estonia (but naturally for Finland as well). Seagoing passengers are a central asset for Estonian tourism, which forms a significant part of the Estonian economy.

Terrorism as a low-probability risk

In the event of a large scale oil accident the consequences could be multiple. The so-called first-order consequences of environmental degradation would be very important and they could extend to economic and even political ramifications e.g. in trying to find who was responsible for the accident. The Gulf of Finland has not yet been faced with a large-scale oil accident. However with the average figure of shipping accidents annually being around 140 and increasing every year, the odds are that a serious accident is bound to happen.

When thinking about the risks of oil transportation at the Gulf of Finland the risk of terrorism does not usually come to mind. However, the possibility exists that a terrorist act could be carried out related to sea transports, especially according to the Russian MA. So far this possibility and probability has not been studied properly (Hellenberg 2006). Risks are becoming increasingly international and complex, and include dimensions concerning strikes in the places never before imagined. Imagination is one of the core attributes that should be exercised in risk mapping and prevention. The central role of oil transports in the region allows the possibility of political tensions, whereas the transportation and their vital role could also be seen as targets for terrorist strikes.

One way of separating the concepts of maritime safety and maritime security is to define safety by incidents caused by natural or technical conditions and security by referring to criminal activities (Baltic Master 2007). Another separation of terms can be the nature of sensitive information. With safety issues transparency is advocated and shared, but with security issues there are often problems of referral to sensitive information. The latter view is apparent in the way the Russians describe the tasks in the region.

In general, the Russian authorities' view of the level of risks in the Gulf of Finland resembles much the concerns of their Estonian and Finnish colleagues. The only noticeable and clearly differing view comes when the security, and not safety, of marine transport is discussed. The Russian view is that one hindrance to deeper safety cooperation, for example to share even greater amounts of information regarding the ships, is the requirements of traffic security in Russia,

which demand classification of part of the information on the ships' cargos and routes. The fear the Russian party expressed was that when giving more precise information about the ships, the Russian MA cannot be absolutely sure that this information stays away from the hands of terrorists. With Russia, therefore, we can clearly see the distinction in defining the concepts of safety and security.

4.4 PRESENT SAFETY SOLUTIONS

Cross-border safety efforts: GOFREP and AIS

GOFREP – the Gulf of Finland Mandatory Ship Reporting System was developed to match the safety needs associated with the rapid growth in vessel traffic. The central idea of GOFREP is to gather information on ships, their cargo and routes, so that the authorities responsible of vessel traffic control (the Estonian, Finnish and Russian MAs) have information on ships navigating in the Gulf of Finland. In addition, the ships that are about to enter the GOFREP area have to report via radio to the operator centre, and the operators can warn and give advice to the ships about various situations (weather, ice, other vessels, manoeuvrable routes etc.) in the Gulf.

In July 2005, a system called the Automatic Identification System (AIS) was launched to give more and precise information about the maritime traffic in the Baltic Sea. The preparation of the system was initiated in 2001 and it is now the dominating automatic system to observe the vessel traffic in the Baltic Sea. The AIS is incorporated into the GOFREP system, but at the moment the information provided through it for vessel traffic operators does not help the operators predict near future traffic situations. The significant amount of information gathered by the AIS is not available to be used in real-time by the operators.

The international waters of the Gulf of Finland, which equals the GOFREP area, has been divided into three areas of responsibility (Figure 10). Southern part and eastbound route (ships entering the Gulf of Finland from the West) are controlled by the Estonian operator centre, the northern route is controlled by the Finnish operator centre and the easternmost strip of international water is controlled by the Russian operation centre. This easternmost strip was annexed into the GOFREP system on the 1st of July 2007.

A large part of the eastern Gulf of Finland is under the jurisdiction of the Russian national vessel traffic service system. When a ship enters national waters it is simultaneously handed over from the GOFREP system to a national Vessel Traffic Service (VTS). The national VTS is quite similar to the air traffic control system, since with the VTS MA (traffic controllers) give not only advice but also commands about movements in national waters.

The northern GOFREP mandated and Finnish controlled route in the Gulf of Finland is very crucial what comes to safety of oil traffic. Full-loaded oil tankers, which have started their voyage from the Russian oil ports in the Karelian Isthmus or St. Petersburg, travel along the coast of Finland, and during winter, in difficult ice conditions. In addition to the Russian part of the route, this lane of the motorway of the seas is the most risky one, due to the criss-crossing of traffic.

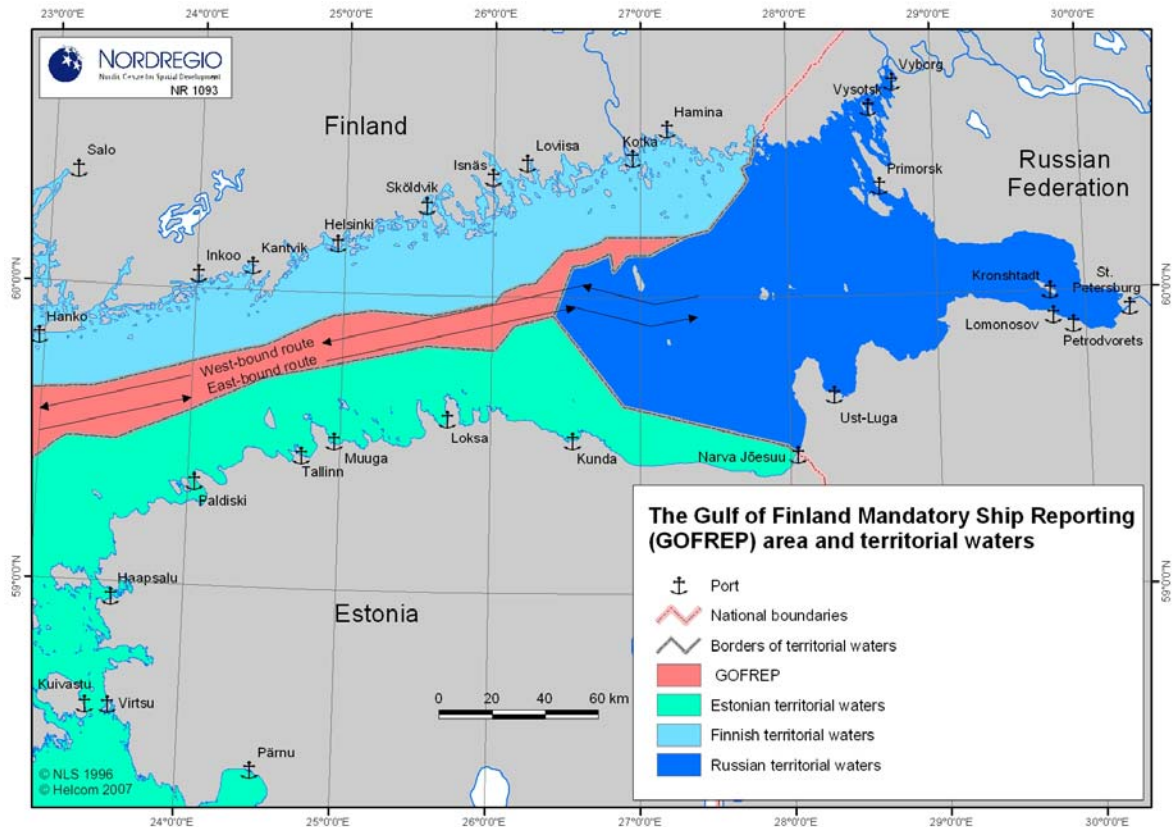


Figure IV—10 GOFREP area and territorial waters.

When justifying the further development of safety-enhancing systems in the Gulf of Finland, the Finnish authorities referred first to the internal safety assessment that they had done in the area. According to the Finnish authorities by using routing systems, risks can be reduced by only 30%, but if reporting, surveillance and traffic control are carried out, risks can be reduced by 80%. Despite this, the accident risk induced by human factors will still remain as high as for 20 %. The ship and its crew are still in a central position to avoid risks and accidents induced by human factors.

The Estonian authorities also said that the AIS and GOFREP systems are the best things that can be done at the moment in order to guarantee the safety of oil transports and marine safety at large in the Gulf of Finland. This reveals the difference between the Finnish and the Estonian authorities' views, since the Finnish more categorically view this phase just as a good *beginning* on the way towards a more comprehensive system.

A central shortcoming of the present system, according to the Finnish authorities, is that the system has merely an advisory role in directing and controlling sea traffic in the Gulf of Finland. The objective of the Finnish marine safety authorities is to develop the system into a sea traffic control system that resembles the one of air traffic in its legal and functional forms. To back this view, the Russian authorities emphasized similarly the fact that despite the newly-introduced AIS and GOFREP systems, the risk level in the Gulf of Finland is getting worse.

Estonian, Finnish and Russian MAs are trying to put forward, through national ministries of transport, and eventually the International Maritime Organization (IMO), a developed version of GOFREP and a common (in contrast

to national) VTS for the whole Gulf of Finland. High hopes exist that this would be operational in the Gulf of Finland in 2008. At the moment, the VTS system is functioning only in national waters, which means that ships entering them are more profoundly under the direct control of the operational centres than the ones navigating in international, GOFREP mandated water. The GOFREP system was taken into use in 2004, and its development was the result of intense cooperation between the MAs of these countries.

The view shared by MAs, especially the Finnish and Russian ones, is that many people were thinking that with the introduction of the GOFREP 'the world would be saved'. However, the national maritime authorities emphasise that the present version of the GOFREP does not abolish risks completely, not even those beyond human factors. Despite the possibility of warning ships, for example those on an incorrect route, it is evermore challenging for the GOFREP operators to follow the vessel traffic situation in the Gulf, simply because of the grown traffic. It has to be stressed that GOFREP is not an intelligent or 'wise' system at the moment.

The above mentioned technical and system-based solutions can evade only part, albeit a big share, of the risks in marine traffic in the Gulf of Finland. The specific winter time conditions (Figure 7 above), especially the difficult ice conditions from January to April, form a central part of risks for traffic in this area. Navigation in ice is difficult, which accentuates the role of the human factor in vessel traffic safety. For example, when vessels manoeuvring in the Gulf of Finland are given the coordinates of icebreakers' routes, the information always refers to a situation that has already passed, thus the open route on the ice might have changed. Heavy vessel traffic also forms queues of ships that line up after ice breakers, which multiplies the risk of rear-end collisions. Risk of collision is the greatest when smaller and bigger ships form these queues. Vessels and tankers of greater tonnage cannot stop in short distances, whereas smaller ones can and do.

All these risks are part of the 20% of risks, induced by human factors, which cannot be erased at the moment by technical solutions and systems. However, the cooperation around safety issues and the establishment of the GOFREP system between Estonian, Finnish and Russian MA has enhanced also this ice manoeuvring safety, despite its above mentioned deficits.

Legislative framework

More agreements usually mean more cooperation. However, different agreements may cause differences in delivery. This has happened in the BSR in such a way that some apply HELCOM recommendations for exemptions, while others apply EU regulations. The Baltic Sea is now surrounded by EU Member States, so it is reasonable to assume that EU regulations and directives will gain more weight. However, since Russia is a major player in the region but not a member of the EU, it is important to hold onto the existing regional agreements and update them to meet the new challenges of the widened EU by anyway following the EU principle of complementarity, i.e. avoiding the duplication of work.

A significant range of European legislation addresses maritime transportation and safety (e.g. Commission 2005a). The European Council is committed to oil spill preventive action, and after the tanker 'Prestige' accident decisions were taken by the European Council aimed at defining the general political guidelines

for the European Union. In the European Union, it is mainly the Transport Council and the Environment Council that are responsible for this action.¹⁰⁹ The establishment of the European Maritime Safety Agency (EMSA) strengthens EU's role in the field of maritime safety and pollution prevention.

After the 2004 EU enlargement Russia remains the only non-EU member state in the BSR, thus ensuring that the Baltic Sea will not form an internal sea of the EU. For this reason it is not possible to rely only on European action and legislation, even if the Commission does consider the transport and energy sectors amongst the most immediate priorities for action (Commission 2006a, p. 9).

The so-called *Helsinki Convention, Convention on the Protection of the Marine Environment of the Baltic Sea Area*, was established in 1992 to protect this marine environment from all sources of pollution through intergovernmental cooperation between Denmark, Estonia, the European Community, Finland, Germany, Latvia, Lithuania, Poland, the Russian Federation and Sweden. The intergovernmental body HELCOM was established to govern the convention, but since then HELCOM has produced many other decisions and recommendations, e.g. the *Copenhagen Declaration on the Safety of Navigation and Emergency Capacity in the Baltic Sea Area* 2001. HELCOM decisions or recommendations are not legally binding, but work almost as legislative instruments, since they are adopted unanimously with a serious endeavour by the parties to comply with them.

In addition, there exist the international conventions of the IMO, which is part of the United Nations administration. The IMO named the Baltic Sea as a Special Sea Area (SSA) in 1995. This translates into several restrictions for e.g. discharges of oil, oily water, oily waste and garbage into the sea as well as for the emissions into the air (IMO 1973/78). Many IMO conventions and resolutions deal expressly with maritime security in the Baltic Sea (e.g. IMO 1972 and 2002; IMO Resolution A 978(24), IMO Resolution MSC 138(76)). Despite the regulations and in direct contravention of e.g. the MARPOL, about 300 operational discharges of oil take place annually (HELCOM 2004).

En-route states with their national legislations cannot bind adjacent nations, and any regulatory and enforcement actions must be consistent with the international law e.g. UNCLOS (United Nations Convention on the Law of the Sea) or IMO Conventions. These regulations, however, do not seem to be enough for coastal states burdened by the increasing traffic, and the likelihood of a major maritime disaster keeps growing.

Most of the recommendations that come from the EU, HELCOM, IALA, EMSA, IMO and other international sea traffic-related organizations are being turned into a binding rule of marine safety procedures. However, the Estonian MA accentuated that problems also arise with the fact that there are so many international organizations with similar or largely overlapping functions, and thus, with similar recommendations to be followed. These organizations are also competing with each other over the question of which of the institutions should get more tasks in maritime safety regulation. Hoarding up these tasks seems to have been a way to justify their existence, which has resulted in a concentration more

¹⁰⁹ The Commission's proposal for a wider EU ban on all single-hulled oil tankers operating in EU waters was agreed upon recently. Internationally the deadline for the phase out for such vessels is 2015.

on the development of technical systems with little value for practical day-to-day work.

The Estonian and Finnish authorities expressed the view that one central problem in putting forward new safety enhancing regulations in this field is the meta-conflict between EU and Russia. A meta-conflict approach is one that can address the many facets of a conflict, be they structural (political or constitutional arrangements, legislation, economic or other factors) or psycho-cultural (attitudes, relationships, divided histories) in a comprehensive and complementary manner (Fitzduff 1989 and 2004). All the regulations and procedures agreed among EU Member States are, one could almost say, naturally contested by the Russians, if such regulations taken as a starting point for marine safety cooperation. It should be mentioned here again that Russian safety regulations are also well developed. Thus, a prerequisite for good EU – Russian cooperation is to use as a point of departure those procedures and regulations that seem to be close to both Russian and European practices. This requires, among other things, knowledge about the way the Russian MA interprets international maritime law and regulations.

Cooperation based on partnership and common will

Hard law comes through the EU and eventually the IMO, but actually the working procedures (traffic surveillance and control) adopted by marine safety authorities of all three countries have been gained through cooperation on the level of professional, practitioners. Thus, the role of regional cooperation is accentuated in enhancing the safety of Baltic Sea energy transportation. It seems that this type of somewhat informal cooperation may be the best way to enhance safety, in the sense that the steps taken towards cooperation are not obliged by the law, but result from practical need. It is therefore evident that a mere top-down approach does not improve the situation, but responding to and moreover anticipating the actual close-call traffic situations do. This is even more apparent when operators have to deal with ships that are operating according to different environmental, technical and social standards.

The hard core of the safety-enhancing system was agreed among marine authorities, although the adoption of the GOFREP system itself is mandated through the IMO. Most procedures that guarantee safety in the Gulf of Finland are based, therefore, on agreed standards of procedure. In this light, the most important feature in safety cooperation in the Baltic Sea is this type of day-to-day joint work between the professional maritime safety authorities of the three countries. As a result, the things agreed in the Document of Joint Procedures, the document of the three MAs to define and describe the things to be done and followed by operators on a very detailed level, go far further than the IMO GOFREP obligation demands.

This is also a tacit criticism of IMO policy, which only concentrates on ship safety itself and not on traffic control systems. The criticism is justified not least because the need for this type of a system that is much more demanding towards ship navigation is also globally evident.

4.5 CONCLUSIONS

Increased traffic density has made oil-related accidents with broad environmental and societal consequences more probable. Many of the experts interviewed referred to internal statistical risk analyses. It is a cause for concern that the estimation is that it is a question of when rather than if a severe oil tanker accident will take place. The maritime safety and security issues need to be given more weight on national as well as international agendas. This was a common view expressed in all the interviews carried out. This motivation has also recently been reflected in the Finnish media (e.g. HS 2007a-d, MTV3 2007, YLE 2007). The following presents the conclusions of the study, which lead to several recommendations on how the maritime safety could be improved.

Combining AIS, VTS and GOFREP

A central innovation in the technical and practical field would be that the vessel traffic operators would have an access to the planned route of vessels in a real time. This implies that a system resembling the vessel traffic service, VTS, in national waters of Estonia, Finland and Russia, combined with the information available through AIS, should be adopted in the whole Gulf of Finland area. In addition, a strict agreement on vessel traffic control procedures should be introduced.

The system would be similar to that of air traffic control. Ships would thus have to follow certain routings, announced in advance, and the maritime traffic control operators would communicate with and monitor ships to ensure they are on their designated routes. The system would also follow the near future situations (vectors of ships) and provide warnings as well as commands to ships if they are about to run to danger. Similarly, the authorities could in advance see if the announced route is suited to the tonnage and other features of the ship.

“Maritime authorities’ responsibilities and rights in traffic control should be widened, i.e. by developing a sea traffic control system similar to air traffic control.”

“The Gulf of Finland and the Baltic Sea could later on act as a pioneer area with this type of use of intelligence system as well as sanctioning procedures to enforce this system, which could later on be imported elsewhere.”

It is therefore clear that all maritime administrations from the three countries would like to see GOFREP developing towards this kind of ‘wise’ system. The worries expressed by the Russian authorities were that at the moment the GOFREP system, with all its data requirements, is too demanding and time consuming. These procedures can divert the attention of ship crews and operators from the main safety tasks of safe navigation. However, these concerns relate to the current and not the fully developed version of the traffic control system envisaged.

In order to create a system of this order we would need the decision by the IMO to make it binding according to international maritime regulations. There are no obstacles to obtaining this, but the bottleneck at the moment is the low standard

of equipment on vessels, such as a lack of e-navigation readiness. Ship owners do not see the need for this equipment, without an IMO obligation even if basically the question concerns relatively inexpensive investments, mainly transponders. The Baltic Sea would act as a very good testing ground in the EU and globally in this matter, since there are already many advanced technical solutions in use, backed up by long-lasting cooperation between the Gulf of Finland states.

In addition, the MA emphasised that a *system of penalties* regarding ships that disregard safety and GOFREP reporting rules should be agreed upon. The restrictions should be severe enough to have an economic effect on ship owners. At present there is no such system, and in order to be effective this type of regulation on pain of sanctions should be enhanced throughout the whole EU. However, by building safety procedures and systems like the GOFREP and VTS, it is possible to cover only part of the 'safety menu' needed for a safe Gulf of Finland. The above-mentioned systems and procedures can diminish the risks entailed by growing tanker traffic but it would not eliminate them. Risk related to human factors and in many cases to the level of professionalism of ship crews, remains at about 20 % of all risks, despite what procedural and technical measures are taken.

A driving licence 'ice passport'

Solving the problem of navigating in dangerous ice conditions needs both political and technical responses and solutions. The view of the MAs interviewed is that the specific geographical context of the Gulf of Finland is not thoroughly understood by the EU authorities, or by the IMO. For the MAs the most worrying issue is not the quality of tonnage, as it was few years ago, but the

"In avoiding risks and accidents it is important to emphasize the role and the know-how of ships' crews."

"The capacities to navigate in ice conditions as well as the security risks should be ensured in sharing information on vessel traffic consideration."

quality and numbers of personnel onboard the ships. However, having a well-qualified crew is a costly business for shipping companies who may decide to prioritize their expenses differently. An ever bigger share of the ships and shipping companies that navigate in the Gulf of Finland are Russian. Taking into consideration the winter-time conditions and the requirements this imposes on ships' personnel it is a positive trend that more ships in the Gulf of Finland are navigated by personnel with experience of winter navigation. For example, it can be speculated that the running aground of the Greek oil tanker *Propontis*, which took place in the Gulf of Finland in February 2007, might have been avoided if its crew had had a deeper knowledge and experience of winter navigation. However, the maritime authorities emphasized that winter navigation training for shipping companies and the crews of the ships would be highly necessary, which would enhance the safety of vessel traffic in the whole Baltic Sea, but especially in the narrow and shallow areas of the Gulf of Finland. Therefore, the need to develop an education and testing system, which was several times referred to as an *ice passport*, is immense. This should be put on the political agenda of EU traffic

authorities, which would in turn develop the issue, including for discussion by the IMO.

Practitioner–level cooperation

Neither safety nor security can be achieved through a one-size fits all approach. It is worth of considering too whether it can be achieved regionally. Despite common goals, safety and especially security measures remain issues that emphasize the sovereign and national decision-making in the globalised world. This analysis has shown that issues of sovereignty still dominate at the higher political level, but that at the more practical (lower) level they do not create an obstacle to deepening cooperation. A perfect example is the development of the GOFREP system.

“In order to best improve safety it is important to enhance cooperation on a professional practitioners’ level i.e. “harmonize by doing”. In addition it is of utmost importance to put this on political agenda, since no progress can be made without a firm political will.”

Considering the risks present in the Gulf of Finland, high marks are due for the cooperation carried out. On such a heavily used sea with high probability of oil accident, the risks are being handled exceptionally well. However, there is a need for political decisions and commitment on the level of IMO and EU, to give a mandate for safety cooperation to evolve further. This mandate would enhance the adoption of existing technical solutions to battle the risks of growing vessel traffic. This is necessary because it is probable that the volume of oil transports will double by 2015. A larger volume of oil transported through the Gulf of Finland will not cause a problem in itself because the size of the ships will increase. But a traffic situation with more and bigger vessels has to be controlled in a much more profound way than is the case today.

However, it would be too simplistic to think that cross-border action only at the level of practitioners is enough. It is important to raise the issues to the international as well as national agendas and get binding instruments e.g. in the environmental protection issues. This should be done in the same cooperative spirit as the operational cooperation.

Afterword

The Gulf of Finland has become one of the risk areas for oil transportation. Taking into account the generally narrow ship routes, due to the shallow waters, as well as winter conditions the probability of collisions and groundings is significant. There are, however, currently several advantages within the area of Gulf of Finland regarding the safety of oil transportation. On the plus side, the fleets sailing in the Baltic Sea are mostly modern. Moreover, transportation with single hull vessels will be a thing of the past by 2010 or at the latest by 2015 and, importantly, the legislation around maritime transportation is strict.

Russia as a central player in the Gulf of Finland and as a global great power wants all decisions to go through the IMO, thus emphasising the UN system rather than the EU system. However, in most cases when Finland and Estonia have tried to operate the system according to EU directives, Russia has *not been reluctant* to

cooperate. This potential barrier to cooperation has been avoided thanks to good and personal contacts with the Russian authorities. Furthermore, it has been especially important that those Russian authorities present at maritime safety cooperation meetings have recently had a full mandate to make decisions. This implies that Russia too has a sincere will to promote safety in the Gulf of Finland. Without this mutual trust and adequate openness, based on common professional background of the people involved, questions that have been negotiated would have easily *turned political*. This would have meant unnecessary obstacles in putting forward important traffic safety measures.

The political nature of practically all cooperation questions with Russia has thus been avoided to that extent that in a *politically sensitive neighbourhood*¹¹⁰, as the region is described in many EU neighbourhood programmes, concrete steps forward have been made possible. It is no surprise that all the parties to the GOFREP cooperation see the present system as globally unique. Barriers of a historical, political and national nature have been overcome by a professional attitude to the questions at hand.

All in all, the Gulf of Finland countries should promote the region as a pilot area within the European Union and worldwide in the field of cross-border risks prevention in maritime transport. This would provide the citizens of the EU in general and particularly the people living by the Gulf of Finland comprehensive safety across their borders and enhance the mutual trust that is needed in developing the safety systems and procedures even further – eventually, towards a traffic control system with high-tech navigation surveillance qualities and traffic command powers delegated to traffic control operators.

¹¹⁰ See the presentation by Chaplinskaya in June 2007 (ISBMS 2007).

CHAPTER V: GAS

Sven Friedrich
and
Jürgen Neumüller

INFRASTRUKTUR & UMWELT

Professor Böhm und Partner

5 NORTH EUROPEAN GAS PIPELINE

5.1 INTRODUCTION

The North European Gas Pipeline (NEGP) is one of the largest subsea gas pipeline projects in the world and is designed to provide EU Member States with 55 bcm natural gas from Russia annually, which will be about 8% of the predicted total gas consumption in the EU in 2015.

The NEGP is by definition a critical infrastructure. The probability of terrorist attacks or natural hazards that could damage or even disrupt the pipeline is rather low. Trawling and vessels anchoring near the pipeline strings pose more of a danger.

The effects of a disruption are local and global. Local effects are gas leakages and a possible gas explosion at sea level. The global effects are possible turbulences in the gas supply and natural gas market, which could burden consumers to a certain extent.

A special issue is the chemical and conventional munitions dumped in the Baltic Sea. Experts suggest that building and operating the NEGP will not cause major risks of releasing chemical warfare agents or explosion of conventional munitions. Nevertheless, this cannot fully be excluded, even if extensive investigations are carried out prior to the laying and operation of the pipeline. These investigations could provide valuable information about the existing risk that should be used in the respective international institutions (e.g. HELCOM) to re-evaluate the risk assessment made 15 years ago.

The Critical Infrastructure Protection strategy should focus on concepts how

- to secure and to safeguard the pipeline mainly against technological hazards as trawling or anchoring ships and
- to have well coordinated and effective emergency response, including the fast detection and repair of damaged parts of the pipeline.

Therefore agreements between the operator *Nord Stream* and the affected Baltic Sea states have to be made. Since the safeguarding work and emergency response touches on the security interests of the states involved, there seems to be a need to develop institutional solutions at political level.

5.2 THE NORTH EUROPEAN GAS PIPELINE

Background

The NEGP is an offshore pipeline under construction from 2005 and 2010 (first line) / 2012 (second line) and operated by *Nord Stream* AG.



Figure V—1 TEN-E priority axes. (Commission 2005c)

The NEGP is planned along one of the priority axes of the Trans-European Gas Networks, the axis ‘Natural Gas 1’ (NG1). This axis leads to the United Kingdom via Northern Continental Europe with connections to Baltic Sea states and to Russia (see Figure 1). Thus, the NEGP constitutes the Baltic offshore part of the NG1-priority axis¹¹¹.

¹¹¹ Although NEGP adheres the EU strategy, there are other possible route options for Trans-European Gas Network axis NG 1. Some states, such as Poland and Lithuania, regard an on-shore pipeline as the ecologically and economically soundest solution. However, Nord Stream fosters the implementation of an offshore pipeline that directly connects Russia to Western Europe for economic and security reasons.

It is designed to supply western European countries such as Germany, the Netherlands and the United Kingdom with 55 billion cubic meters of natural gas annually, mainly obtained from the Shtokman gas field in the Barents Sea (overall reserves have been estimated for 3.7 trillion tons).

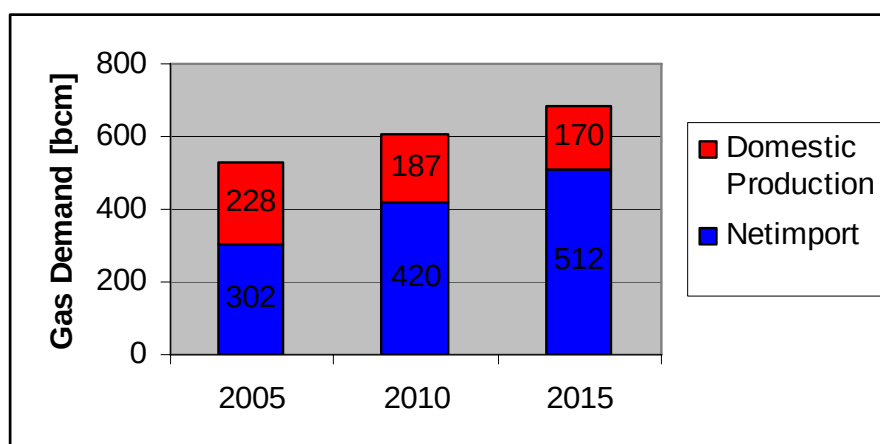


Figure V—2 Projection of gas demand in the EU.

According to a baseline scenario, the demand for natural gas is expected to increase between 2005 and 2015 from 530 to 682 billion cubic meters, whereas the domestic production will decrease from 228 billion cubic meters in 2005 to 170 billion cubic meters in 2015, creating an additional need to import 210 billion cubic meters natural gas in 2015. *Nord Stream* could provide about 25% of the natural gas needed (Nord Stream 2006a).

Technical design

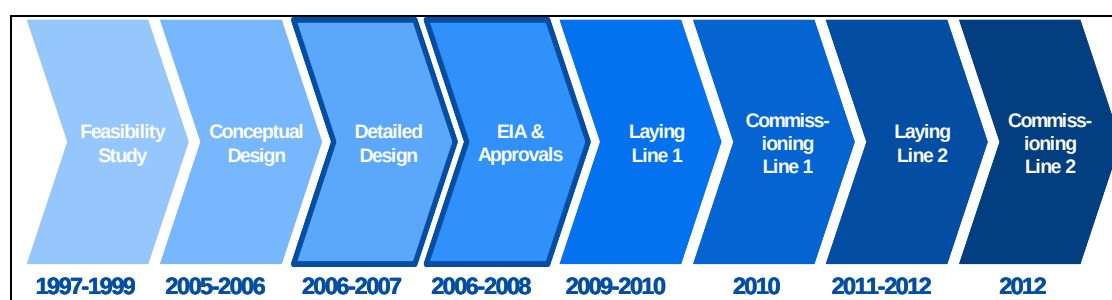
The NEGP will have a total length of about 1,200 km, making it one of the longest offshore pipelines in the world. It will start from Portovaya Bay near Vyborg, Russia, and then run along of the Baltic seabed until it reaches its landfall in Lubmin, near Greifswald, Germany. It will cross the Exclusive Economic Zones (EEZ) of five countries: Russia, Finland, Sweden, Denmark and Germany (Nord Stream 2006a and 2007a). The NEGP will be laid in depths ranging mostly from 20 m to 100 m, being at deepest in 210 m.

According to plans, there will be a service platform located in the Swedish EEZ, about 48 km east of the small island of Gotska Sandön, and 68 km northeast of the main island of Gotland. Service platform's main functions are told to be commissioning support, operational support/maintenance of the pipelines, providing flexibility in case of an operational problem and isolation in case any of the pipelines are damaged. The platform will be unmanned, with the exception of temporary maintenance workers. The service platform will be about 40 m long by about 30 m wide, with the height of the main structure above the surface of the sea about 40 m. It will not be visible from any point on land. (Nord Stream 2007b)

According to latest information from *Nord Stream* (2007a), the project preparation phase entered into a detailed planning phase on 1 January 2007. The start of the main construction is scheduled for the third quarter of 2008 and will be finalised in 2010. The second line is expected to operate in 2012.

Table V—1 Intersections of Nord Stream with exclusive economic zones and territorial waters in the Baltic Sea. (Nord Stream 2006a)

Country	EEZ (km)	TW (km)	Total (km)
Russia	96	22	118
Finland	369	0	369
Sweden	482	0	482
Denmark	149	0	149
Germany	33	45	78

**Figure V—3 Milestones for the NEGP-project. (Nord Stream)**

State of permission procedure

According to the 1982 United Nations Convention on the Law of the Sea (UNCLOS), the Exclusive Economic Zone (EEZ) falls under national jurisdiction. This covers the construction and operation of pipelines (UNCLOS 1982). The consortium *Nord Stream* is therefore obliged to obtain all necessary permits according to the national law that applies in the EEZ crossed by the NEGP.

The necessary permits demand an Environmental Impact Assessment (EIA) for each of the EEZ as well as for Territorial Waters (TW) crossed by the NEGP. In addition, the construction and operation of the NEGP is subject to the “Espoo Convention on Environmental Impact Assessment in Transboundary Context”, since the construction of “large-diameter oil- and gas pipelines” is regarded to “cause a significant adverse transboundary effect” (EC EIA 1991, Annex I, no. 8). This means that all parties of the convention have to be notified about the EIA procedure to be given the opportunity to participate in the respective EIA procedures.

In case of the NEGP, the parties of origin (meaning those states whose EEZ or TW are crossed by the planned pipeline and who are responsible for EIA-procedures) are Russia, Finland, Sweden, Denmark and Germany. They notified the affected parties, which are all the states of the Baltic Sea Region, about the nature of the planned measure. The affected parties indicated their desire to participate in the relevant EIA-processes.

Fact Box V—1 Basic and technical facts of the NEGP.

Route	Subsea pipeline from Portovaya Bay near Vyborg, Russia to the coast of Germany to Lubmin near Greifswald, Mecklenburg-Western Pomerania.
Service platform	In the Swedish EEZ, about 48 km east of the small island of Gotska Sandön, and 68 km northeast of the main island of Gotland. The size of the service platform will be about 40 m x 30. The height of the main structure above the surface of the sea will be about 40 m.
Constructor	Nord Stream AG http://www.nord-stream.com
Shareholders*	OAo Gazprom (51%), Wintershall AG (24.5%), E.ON Ruhrgas AG (24.5%)
Estimated investment	min € 5 billion
Gas capacities	55 bcm per annum (2 pipelines with 27.5 bcm capacity each)
Pipeline length	1198 km
Max. water depth	210 m
Project start	2005
Completion of the first line	According to plan – in 2010
Completion of the second line	According to plan – in 2012
Pipeline diameter	1,220 millimetres / 48 inches
Design pressure	220 bar
Pipe steel standard	DNV Offshore Standard OS-F101; Steel grade: X-70
Wall thickness	27-41 mm.
Coating	Interior antifriction coating of 0.06 mm epoxy layer; Exterior anticorrosive PE or PUR coating; Passive anticorrosive protection is ensured by aluminium sacrifice bracelet anodes
Gas supply resources	Yuzhno-Russkoye oil and gas reserve, Yamal Peninsula, Ob-Taz bay and Shtokmanovskoye fields

* Dutch gas infrastructure company N.V. Nederlandse Gasunie has agreed in November 2007 with Russian Gazprom the principal terms and conditions for its participation “in the near future” in the *Nord Stream* consortium. Gasunie will get a 9 per cent stake in the joint venture. Gazprom will keep its 51 per cent stake and the German companies E.ON Ruhrgas and BASF/Wintershall will hold 20 per cent each, that is, E.ON Ruhrgas and BASF/Wintershall will each cede 4.5 per cent to Gasunie. (Nord Stream 2007)



Figure V—4 Route of the pipeline proposed by Nord Stream.

The EIA has to be elaborated by *Nord Stream* before decisions are made, and it includes public consultation where affected parties may participate. The procedures as well as the content of EIA differ between the parties of origin.

Taking the German EIA procedure, it is expected that the results of all EIAs will provide essential information on risks connected with construction and operation of the NEGP. However, they might not cover all information relevant for Critical Infrastructure Protection (CIP) issues as following chapters will show. (See Fact Box 2)

5.3 THREAT SCENARIOS

Both the “Proposal for a Directive of the Council on the Designation and Identification of European Critical Infrastructure and the Assessment of the Need to Improve their Protection” (Commission 2006a) and the “Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight Against Terrorism” (Commission 2004) classify “energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)” as critical infrastructure. The following threats are examined here:

- Terrorism-related hazards
- Natural disasters
- Hazard from dumped munitions
- Other hazards

Terrorism-related hazards

Pipelines have been targeted for terrorist attack, although there are no known successful attacks on underwater pipelines (Australian Office of Transport and Security 2004).

Nevertheless, terrorist attacks on offshore oil and gas facilities have taken place, such as the repeated attacks on Nigerian offshore oil-platforms (FOI 2007).

Attacks on or accidents at on-shore pipelines are frequent, mainly in critical hot-spots. Pipeline systems are strategic goals of terrorists and rebels, such as in Iraq, Pakistan, Nigeria, Assam, Chechnya and Kurdistan (IAGS 2005).

Attacks and accidents can disrupt oil or gas transmission. The media and energy market is sensitive to bad news, as has been demonstrated recently with the explosion that damaged a Ukrainian pipeline (Der Tagesspiegel, 7 May 2007). Experts talk of ‘fear premium’ that is added to gas and oil prices. According to the Institute for the Analysis of Global Security this ‘fear premium’ makes up about 10 US\$/barrel oil (IAGS 2005).

Fact Box V—2 Permission procedure for NEGP in German EEZ and TW.

On 11 November 2006 *Nord Stream* applied for permission of construction and operation of the pipeline in German EEZ and TW at the Bergamt Stralsund (Federal Mining Agency Stralsund, subordinated to the Mecklenburg-Vorpommern Ministry for Economic Affairs, Labour and Tourism) as well as at the Bundesamt für Seeschifffahrt und Hydrographie (Federal Maritime and Hydrographic Agency, BSH).

The BSH states in its notification in accordance with Article 3 of the Espoo-Convention (EC EIA 1991), that three different permits are required for the construction of the pipeline (BSH 2006):

- “1. According to § 43 Energy Trade Law, a planning approval by the Federal Mining Agency Stralsund is needed for the section of the pipeline in German Territorial Waters.
2. According to § 133 fig. 1 Federal Mining Law, an approval with regard to technical and safety aspects by the Federal Mining Agency Stralsund is required.
3. According to § 133 fig. 2 Federal Mining Law, an approval with regard to the use of the waters and environmental aspects by the BSH is required.

An EIA is obligatory for decisions fig. 1) and 3).”

The application of *Nord Stream* included a scoping document, where the potential environmental impacts of the measure as well as the proposed assessment of the environmental impacts are described (Nord Stream 2006b).

The responsible authorities, the BSH and the Bergamt Stralsund jointly decided upon the methodological framework for the EIA.

According to this decision the EIA will touch concerns of CIP in some points, e.g. (BA Stralsund / BSH 2007):

- a description of effects of damages to the pipeline by external impact which could be terrorist attacks or natural disasters,
- a small-scale investigation (side scan sonar) and a large-scale investigation (magnetometer) of dumped munitions for the entire track; both approaches should cover at least 15 meters width,
- an assessment of the effects of possible clean-up of munitions,
- an assessment of the effects of a sudden gas leakage to the coastal population.

National bodies responsible for security issues and security experts see a general possibility for terrorist attacks against offshore gas infrastructure. Each method of attack used in the following scenarios involves a high degree of difficulty given the location, size and complexity of the infrastructure (Australian Office of Transport and Security 2004):

- Direct attack
- Armed intrusion
- Hijacked vessel/aircraft
- Sabotage
- Underwater attack

The extended and isolated nature of the pipelines from offshore facilities make it practically impossible to guard them. However, the threat to offshore pipelines is reduced by the depth at which they traverse the seabed, thereby presenting a significant difficulty for would-be attackers (Australian Office of Transport and Security 2004).

However, security experts regard a pipeline as a fairly vulnerable object, where one diver would be enough to set an explosive device (FOI 2007).

Generally, the likelihood of a terrorist attack is regarded as rather low, since the political situation in the Baltic Sea Region is stable. Nevertheless, experts reckon that there are threats to Russian interests and citizens. If the current trend continues, the situation will worsen and, because the pipeline is meant to be in operation for five decades, a high level of uncertainty must be reckoned with (FOI 2007).

Natural disasters

Generally, seismic events, tsunamis, rough sea with strong swells, onshore winds, and storms could affect a subsea pipeline. Problems are also created by buried subsea pipelines becoming exposed, particularly after violent wave action associated with storms. This may cause stability problems or free spanning, which are both potential hazards for the pipeline (Pipeline and gas journal 2000). The landfall pipelines are exposed to the risk of rockfall impacts and the ice cover of coastal area (Nord Stream 2006a).

Experience from the Gulf of Mexico shows that pipelines on the seabed suffered only minor damage after major hurricanes; most damage affected platforms and risers leading from bottom pipelines to the surface and for pipelines up to a depth of 60 meters (DNV 2006).

In North Sea, sea storms have been known to expose pipeline trunks, which leads eventually to larger free spans and thus more stress on the pipelines (Bijker 2000).

For NEGP, sea storms, rockfall and ice cover come into question, since seismic events or tsunamis are unlikely in the Baltic Sea Region.

Dumped munitions

A special point in discussion is the history of the Baltic Sea as a dumping ground for chemical and conventional munitions. The interaction between *Nord Stream* and the dumped munitions seems to constitute a specific threat scenario.

After the first and second world wars tens of thousands of tons of conventional and chemical munitions were dumped at different places in the Baltic Sea.

Dumped chemical munitions in particular were subject to investigations by the Baltic Marine Environment Protection Commission (HELCOM). The Ad Hoc Working Group on Dumped Chemical Munition (HELCOM CHEMU) states in its "Report on Chemical Munitions dumped in the Baltic Sea" of January 1994, that "about 40,000 tons of chemical munitions including 13,000 tons of warfare agents have been dumped" in the Baltic Sea (HELCOM CHEMU 1994). But according to figures provided by the German BSH, 58,300 tons of chemical munitions were dumped east of Bornholm alone (Nehring and Ilschner 2005). Other sources also assume that the amount of chemical munitions dumped in the Baltic Sea is higher than stated in the before mentioned report of the HELCOM CHEMU working group (MoND 1999). Investigations by a Russian specialist team revealed that corrosion of dumped chemical munitions trunks has advanced dramatically and that the Baltic seabed contains 3 grams / kilogram of arsenic (Berliner Salon e.V. 2007, Paka 2007).

Closely related to the dumping of chemical munitions is the dumping of conventional munitions (which took sometimes place simultaneously) and the appearance of mine belts in Baltic Sea coastal waters.

Dumped conventional munitions have not been investigated so far. There are only uncertain figures in the scientific literature. It is estimated that from Schleswig-Holstein's harbours alone 100,000 tons of conventional munitions were dumped in the Baltic Sea (Nehring and Ilschner 2005).

There was extensive mining of the Baltic Sea area during World War II. Apart from German, Russian and Finnish minefields, there were also Swedish and British minefields. According to the literature, about 120,000 sea mines were laid between 1914 and 1945. Although some have been cleared, others are still active, especially along the southern Baltic coast and in the Gulf of Finland (Nehring 2006).

Nord Stream's strategy is to investigate the line corridor for dumped munitions, to avoid dumping sites by alternative route design and to clean-up dumped munitions where necessary and possible. In 2005, 2006 and 2007 *Nord Stream* carried out investigations of the seabed. The first detailed screening of *Nord Stream's* provisional route was carried out by PeterGaz in 2005. This was principally a geophysical survey to check the condition of the seabed across a 2 km corridor and to look for obstacles such as wrecks, large boulders and trenches.

On the basis of the 2005 survey data, two potential pipeline routes were selected. These were investigated in 2006 during a second seabed survey, which covered a 180 metre-wide corridor along the entire length of the proposed pipeline. *Nord Stream* then deployed a remotely-operated vehicle (ROV) to inspect each target in detail within 20 metres of the route. As a result of the 2005 and 2006 surveys, only two targets were clearly identified as mines and only one is thought to be intact.

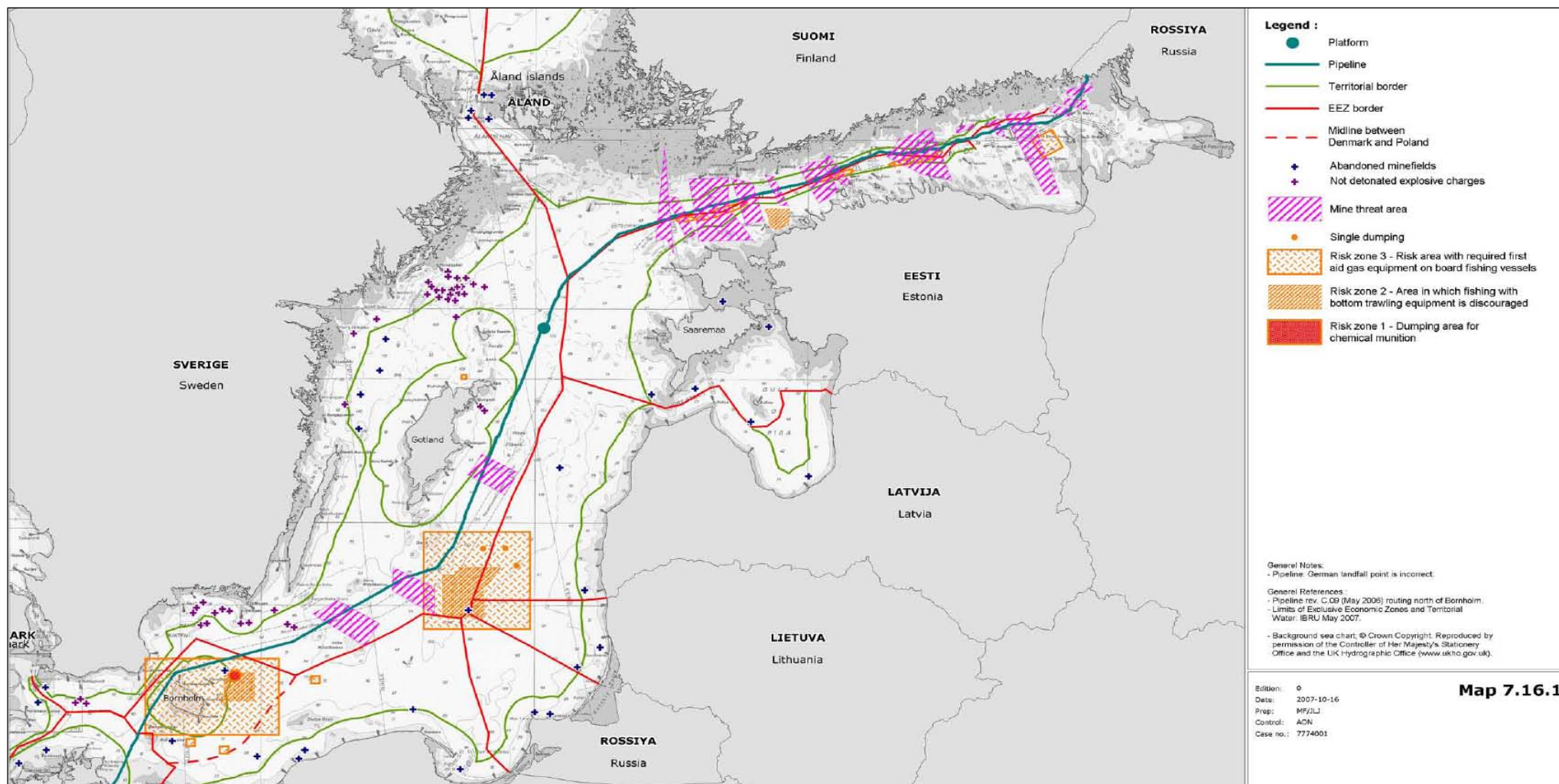


Figure V—5 Dumped munitions in the Baltic Sea. (Nord Stream)

Since July 2007 a three-step approach is being applied. In the first stage the installation corridor (15 metres) is surveyed with multi-beam echo sounders (MBES), high-resolution side-scan sonar's (SSS), sub-bottom profilers and magnetometer. In the second stage a 6.7 metre-wide 12 sensor gradiometer array mounted on a ROV is used to detect any ferrous (iron-based) metals on the seabed and in the third stage, objects detected in the previous stages will be visually inspected.

Other Hazards

Additional threats to sub sea pipelines are mentioned in the literature as being anchoring, trawling and fishing. Trawling or the anchors of drifting ships may cause damage, e.g. moving the pipelines or disrupting them. For this reason, some countries like Australia or New Zealand even prohibit anchoring and fishing in designated pipeline corridors (Burnett, 2006).

The probability of such incidents to subsea pipelines is regarded much higher than the probability of terrorist attacks or natural hazards. Damage to pipelines caused by vessels (anchoring, running to the bottom) has been estimated to be once per 237 years (Mazurkiewicz 2007).

5.4 IMPACTS CAUSED BY TERRORISM, NATURAL DISASTERS AND DUMPED MUNITIONS

The following chapter describes the impacts resulting from direct pipeline damages as well as impacts caused by the construction and operation of the pipeline.

Natural disasters and terrorist attacks may cause direct damage to subsea pipelines by moving them out of position, interrupting or damaging them in a way to cause a gas leak. The worst case of a direct impact is certainly the total disruption of the pipeline. Other direct damage could be the damaging of landfalls and pressure stations.

Due to the situation in the Baltic Sea with regard to dumped munitions, further indirect effects of the construction of the pipeline are imaginable: dumped munitions could explode during construction or warfare agents could be released due to construction work (damage to munition trunks) or increased corrosion caused by the removal of sediment and exposure of metal trunks to salt water.

People at risk

Direct damage to the NEGP will most probably result in impacts that are locally limited and affect single groups of persons rather than have a greater impact on people. However, it seems it cannot to be excluded that leaking gas could cause vessels to sink, maybe even tankers with hazardous load, either by an explosion or due to a large gas bubble, such as described by Hupka (2007).

Unexploded ordnance, such as bombs, grenades or sea mines, could harm the crew of a ship near the explosion. In 2005, three Dutch skippers were killed by a mine explosion. From the available literature it seems that there is not enough knowledge about the behaviour of dumped conventional munitions over time. For

example it is point of contention whether munitions deactivate due to corrosion or if self-ignition is likely. There may be a severe risk to pipeline workers, since digging and dredging could cause an explosion near to a pipeline construction vessel.

Up to now, the warfare agents released from chemical munitions dumped in the Baltic Sea have not cause fatal casualties. Nevertheless a number of fishermen have been injured, mainly by mustard gas munitions caught in their fishing nets. Danish records show 342 chemical munition incidents between 1985 and 1992 east of Bornholm (HELCOM 1994) and around 100 incidents between 1995 and 2005. There was a tragic accident in 1955 in Poland when 102 children were injured when they played with a mustard gas munition washed up on a beach near Darlowek. The impact of mustard gas is severe and takes a long time to recover from exposure to it (MoND 1999). Statistics from Denmark indicate a certain decrease in munitions incidents during the last two decades, but those statistics do only represent a part of the munition incidents, since foreign fishermen are not obliged to report to Danish authorities.

“If the pipeline is punctured or torn apart, it will take some time before the pressure fall is registered at the landfalls at compressors and at the service platform and the security system automatically closes the valves of the pipeline. The gas will bubble into the water and reach the sea level. From there the gas will spread in the atmosphere depending on the meteorological conditions and the weight of the gas in relation to the surrounding air, etc. In connection with the release of gas, the gas will cool down, and may become heavier than the surrounding air. However, in connection with the rise of the gas plume in the water the gas will be heated up and it is expected that the gas when reaching the sea level will be lighter than the surrounding air. Thus, no heavy gas cloud will be formed at sea level. The gas will most probably disperse into the atmosphere. If the ignition source is onboard a passing ship, or on board the ship that has caused the rupture/leakage (anchor damage), there will be a risk to the personnel onboard the ship. This risk will be further evaluated at a later stage of the project. It should be mentioned that an accident with outlet of gas will be very rare with a frequency, calculated for the planned Baltic pipeline, which corresponds to an accident once in about 1,000 – 10,000 years”.

Fact Box V—3 Effects of a gas leak on the NEGP. (Nord Stream 2006a)

For other warfare agents, such as Clark I, Clark II, adamsite, lewisite and winter sulphuric yperite accumulation of arsenic in biosphere cannot be excluded. Whether the decomposition will create non-toxic substances is not fully understood (MoND 1999, Kasperek 2007).

The risk to people, either from direct damage to the pipeline or by indirect impacts during the construction and operation of the pipeline seems highest for specific groups, e.g. fishermen, ship crews and pipeline workers.

A general impact on a greater number of people seems rather improbable. But it could happen that a gas leakage could cause major accidents involving tankers or ships with hazardous loads.

There seems to be rather low evidence for the assumption that the construction and the operation of the NEGP could significantly worsen the current situation concerning dumped chemical munitions since the NEGP is limited to a narrow corridor and extensive investigations are carried out prior to construction.

Table V—2 Pull-outs of chemical munitions east of Bornholm registered by Denmark.¹¹²

Year	Number of catches	Weight of chemical munitions in kg	Weight of active gas in kg
1985*	46	2695	
1986*	41	1830	
1987*	14	582	
1988*	19	1044	
1989*	42	1966	
1990*	19	979	
1991*	103	5378	
1992*	58	2597	
1993			
1994			
1995**	6		40
1996**	10		210
1997**	9		184
1998**	5		290
1999**	3		185
2000**	11		512
2001**	11		514
2002**	10		345
2003**	25		1110
2004**	4		160
2005**	4		105

¹¹² Sources: *: HELCOM 1994, **www.helcom.fi (16.10.2007).

Economic consequences

Gas leakage and the resulting reduction of gas delivery will first of all result in lower revenues. The direct economic damage from a gas leakage of one of the pipelines depends on the severity of the damage and the time it takes to detect and repair the leak. Given a complete interruption, an annual discharge of 27,5 Bcm (daily discharge at 75,000 Tcm) for one string and an average price level it would create revenue losses of about 10 to 20 million EUR/day, which is substantial.

The Australian Office of Transport and Security states that a terrorist attack could weaken international confidence and damage future foreign investment in Australia's energy industries. Indirect effects could include short-term oil price instability; pressure on joint offshore development and security arrangements between Timor-Leste and Australia; potential reluctance to work on offshore facilities; attendant bad publicity; and the imposition of additional security and hiring costs to operators of offshore-related or maritime-related enterprises (Office of Transport and Security, Australia 2004: 12-13).

When considering indirect economic damage, one has to bear in mind that only the transfer of gas would be affected, not its production. The impact of the gas cut in January 2007, when Russia stopped its delivery to Ukraine, did not greatly affect the European economy. This was mainly due to the combination of availability of storage capacities, the activation of other supply chains and the warm winter. The consequences of a shut-down of the NEGP should be regarded in light of its contribution to gas supply. The gas supply via the NEGP will account for about 11% of total imports from Russia to the European Union, whereas imports via Ukraine make up two thirds of European gas import from Russia. So called 'fear premiums' could hit mainly the consumers in Western Europe by temporarily rising gas prices.

The direct economic damage resulting from contamination by toxic warfare agents should be rather moderate since it has mainly local effects. Indirect economic impacts connected to a worsened public image of coastal Baltic Sea regions if accidents with dumped munitions are reported more frequently are unlikely. It has not yet been investigated whether the decomposition of dumped munitions due too corrosion could lead to accidents in coastal areas where especially the tourism and fisheries sectors could suffer losses. Nevertheless there have been accidents reported previously in that media (e.g. ZDF 2005) and it was stated that white phosphorus has been released due to a geological survey in the coastal waters near Usedom (AET 2007). It is however rather questionable whether the NEGP will cause such effects since extensive surveys are carried out prior to laying the pipeline. Paka (2007), states that other hydrotechnological investments (e.g. subsea cable) did not worsen the situation of released warfare agents.

Environmental damage

Responses to the proposal of *Nord Stream* regarding the Environmental Assessment for Finnish / German EEZ revealed major concerns that are related to the construction of the pipeline (BA Stralsund / BSH 2007, Finnish Ministry of the Environment 2007):

- Impact on the Natura 2000 network

- Impact on fish stocks and bird life
- Alteration of the seabed
- Dumped munitions and ship wrecks

These are mainly related to the construction phase of the pipeline, and in this case the impact is limited in time. Concerning biota, the greatest concern is the impact on fish-stocks and on bird species due to disturbance during the construction of the pipeline. The seabed could be negatively influenced by necessary construction works, dredging, filling and blasting. Sediments could be disturbed as well as local sea currents. Fine sediments could be shifted abroad; harmful substances contained in the sediment could be released.

The comments (especially from Finnish authorities) to the proposed Environmental Assessment show clearly that there are substantial concerns. Finnish authorities therefore wish to model long-term risks mainly connected to sedimentation and the release of harmful substances to better evaluate associated risks.

Concerning chemical weapons, the project “Modelling Ecological Risks related to Sea-dumped Chemical Weapons” (MERCW) is being carried out within the 6th Framework Program by the Finnish Institute of Marine Research. No final results are yet available.

Another issue that up to now cannot be fully judged is the question of conventional munitions and release of harmful substances such as heavy metals from corroded bombs. It seems that the possible environmental impacts have not yet been assessed sufficiently, and it may be assumed that the construction of the pipeline will alter environmental conditions. On the basis of available information it cannot be said whether the construction of the pipeline will have indirect effects, such as enhancing the corrosion of chemical and conventional munitions leading to a faster release of toxic or harmful substances. It is also unclear how the warfare agents will behave once set free in larger proportions.

5.5 CRITICAL INFRASTRUCTURE PROTECTION STRATEGY

Although the probability of attacks and natural disasters that could harm the NEGP is rather low, the effect of this could be substantial taken the importance of the pipeline (the NEGP will provide 8% of the total European gas demand) and the side effects concerning dumped munitions. Therefore, in a Critical Infrastructure Protection strategy (CIP strategy) hazard scenarios should be described and responsibilities for prevention and mitigation of the hazards should be defined.

In case of the NEGP the CIP Strategy should address following issues:

- Securing the NEGP against trawling and anchoring vessels.
- Safeguarding of the most vulnerable parts of the NEGP (landfalls in Vyborg and Lubmin as well as the service platform).
- Emergency response and repair of damage to the pipeline.
- Avoidance of side effects of building and running the NEGP related to dumped munitions.

Political dimension

Even if the NEGP is seen as a private sector activity, its strategic role in gas supply for the European gas market and the fact that it runs through the EEZ of five Baltic Sea states makes it a political issue. Several individual issues have been raised, which create conflicts. Thus, the plan of *Nord Stream* to erect a service platform next to the Swedish island of Gotland followed an intensive public debate in Sweden. A major concern was possible intelligence collection by Russia. This debate was fed by a statement by Vladimir Putin who said in a TV interview that the Russian fleet's "role is to protect our economic interests in the Baltic Sea region [...] Protecting the Northern European Pipeline, which brings energy resources to our Western European customers, is one of our most important priorities" (quoted from Pursiainen 2007). Later, *Nord Stream* has tried to build confidence especially as to the use and protection of the service platform by stating that "in case any surveillance is needed, it is the responsibility of no one else but the Swedish Coast Guard" (Nord Stream 2007b).

Major concerns about the NEGP have been expressed by Poland, whose Minister of Defence stated that "Poland has a particular sensitivity to corridors and deals above its head. That was the Locarno tradition and the Molotov-Ribbentrop tradition. That was the 20th century. We don't want any repetition of that" (quoted from Pursiainen 2007). The importance of the issue is shown by the fact that the Polish parliament (Sejm) organised an international conference in May 2007 to discuss the issue with experts (International Conference on Environmental Threats to the Baltic Sea, Warsaw, 28 May 2007).

It is important that those states affected by the NEGP would find a common ground at the political level. Even if the United Nations Convention on the Law of the Sea (UNCLOS)¹¹³ clearly states that the pipeline operation should not be impeded, additional efforts about the relevant security issues are needed.

Institutional dimension

Nord Stream is responsible for operating the NEGP and principally *Nord Stream* should have highest interest in developing and implementing a CIP strategy for NEGP in order to avoid economic losses. To avoid these losses, it has to be assumed that *Nord Stream* will take care of detecting pipeline damage continuously and the fast repair of damaged parts of the pipeline.

More complicated is the field of safeguarding and complex reactions in emergency responses that might be necessary in rare cases. Even if the risks mentioned above are low, the safeguarding of a pipeline that crosses the Baltic Sea at a length of 1,200 km is a multinational task. There must be a sound strategy developed together with experts from the affected states that concentrates on crucial points such as landfalls or pressure stations.

¹¹¹ UNCLOS; Article 210: According to UNCLOS, pollution resulting from dumping shall be prevented by the responsible coastal state. Article 79: According to UNCLOS, all states are entitled to lay pipelines on continental shelf, coastal states may not impede the laying or maintenance of such cables or pipelines

But first it has to be clarified who is responsible for safeguarding the pipeline (national coast guards, private security services, national intelligence agencies). Many mainly operational questions follow:

- By which means and what information will be gathered?
- How this information will be stored and analysed?
- Will it be partly shared between involved security operators (intelligence agencies)?

Secondly, it has to be clarified who is responsible for emergency responses (national coast guards, private services, *Nord Stream*), as well as who, and in what cases, will lead the emergency response action? Of course, reaction plans and trainings are essential. In order to find the way forward, and keeping in mind that the CIP of the NEGP has a political dimension, it seems advisable that the CIP strategy be developed and implemented by a broader panel comprising security experts and political decision makers.

For this purpose existing bodies, such as the Council of the Baltic Sea States (CBSS), should be considered to see whether they could moderate the process. It would also be possible to establish a separate – intergovernmental/interadministrative – working structure.

Another special issue is the dumped munitions, which extend beyond the NEGP. Being part of the CIP strategy for the pipeline track it should be discussed comprehensively in a broader forum, already established in HELCOM. It is essential that all available information concerning the investigation of dumped munitions is made available to HELCOM and that, based on an actual evaluation of the potential risks, the need for further action is decided at a political level.

Economic dimension

Since the most significant effect of a pipeline disruption could be turbulences in gas markets, CIP has to find solutions for securing gas supply by either re-routing the supply via other pipelines or assuring enough storage volume to overcome a period lasting from several days to several weeks. The costs for securing and repairing the NEGP are presumably small in comparison to the revenue loss, should the pipeline be disrupted. Therefore the protection of the NEGP should be a clear task and in the interest of *Nord Stream* and the consumers that benefit from it.

Social dimension

The CIP has to be directed mainly to those groups and people that would be most directly affected by accidents along the pipeline, such as fishermen, ships' crews as well as pipeline workers. The NEGP could also support information campaigns to people living along the Baltic Sea coast about what to do in case of accidents involving dumped munitions.

Technological dimension

The CIP should take into account two aspects: the technological opportunities in safeguarding using new technologies (cameras, satellites, sonar) as well as the

vulnerabilities of pipelines to attack, which is why the access by terrorist groups to technology have especially to be continuously monitored.

CHAPTER VI: WATER

Birgitta Backman, Samrit Luoma,
Philipp Schmidt-Thomé
and Jukka Laitinen

Geological Survey of Finland

6 POTENTIAL RISKS FOR SHALLOW GROUNDWATER AQUIFERS IN COASTAL AREAS OF THE BALTIC SEA: A CASE STUDY IN THE HANKO AREA IN SOUTH FINLAND¹¹⁴

6.1 INTRODUCTION

The threats concerning shallow groundwater aquifers or water supply infrastructure are much the same all over Finland, but the coastal area aquifers face, in addition, specific threats caused by their location on the seashore. The Hanko aquifer, located in the southwest coast of Finland, was used as a case study area for the evaluation of the potential threats for the use and management of groundwater resources and water supply. Threats and risks to groundwater quality and quantity, caused by human activities or climate change, were identified.

The specific risks and threats to a seashore aquifer are changes in present sea water level, contamination of salt-water intrusion, and future sea level rise and change in precipitation and evaporation caused by climate change. Groundwater level monitoring data in two observation wells of 30 minutes intervals and the sea level monitoring data of 60 minutes intervals were produced in the Hanko case study area.

Based on this data, it was observed that the sea level changes have a direct and very fast effect on the groundwater level. The effect was worse in that part of the Hanko aquifer where the permeability of sand and gravel layers was high. According to the climate change scenarios, the significant rise of sea level in the Hanko coastal area could cause problems to the water supply managements and infrastructure planning in the Hanko and in many other coast aquifer areas. The study has proposed a conceptual model for protection of shallow groundwater aquifer for the Hanko and other coastal areas aquifer.

Global groundwater

Groundwater is water located beneath the ground surface in soil pore spaces and in the fractures of bedrock. Beneath the water table all the pores and fractures are fully saturated (Freeze and Cherry 1979). A unit of bedrock or an unconsolidated deposit is called an aquifer when it can yield a usable quantity of water. The Earth is covered to 70% by water; most part of this water is, however, seawater. The freshwater is mainly bounded in glaciers and only about 1% of all water resources

¹¹⁴ The authors would like to thank the following persons: Kimmo Paakkonen, the Hanko Water Work and Timo Kinnunen, Uusimaa Regional Environment Centre for contributions of the Hanko groundwater data; Professor Reijo Salminen for review of the manuscript and for his constructive comments and advices; Arto Pullinen for his help in the fieldwork.

are groundwater. The global water balance is very sensitive and even small changes, for example in atmospheric temperature may affect it. The groundwater state is usually more stable than surface water state is and is better protected against different risks than surface water, for example contamination. There are, however, a lot of risks also for groundwater, both on its quantity and quality.

Sustainable development in the use of renewable groundwater resources requires that the pumping of groundwater does not exceed the recharge. Over-pumping of groundwater resources has happened in tracts of China, the Middle East, North Africa, Saudi Arabia, and the U.S.A. and the groundwater table has decreased alarmingly in these areas. Globally, the use of freshwater has tripled in the last 50 years. The greatest consumption of water is by agriculture, about 70%, by industry, about 22% and by cities and communities only 8% (Rankila 2007). It has been assessed that globally after 20 years more than 65% of inhabitants will face shortages of freshwater. The demand for freshwater has a great conflict potential, e. g. in the Middle East.

In some areas groundwater resources are at risk from the results of human activities, and an increase in population can cause the overuse and contamination of groundwater resources, which consequently affect major infrastructure and water management. Moreover, climate change currently leads to a further warming of atmosphere and may cause changes in the global climate system in the near future. This change would directly affect the groundwater resources, due to changes in global temperature, precipitation and floods patterns, as well as the global mean sea level rise. In conjunction with higher water demand and increasing pollution due to increasing populations, this would cause a crisis to groundwater resource management strategies and infrastructure planning.

Groundwater resources in Finland are mainly restricted to Quaternary deposits but are found to some extent in faults and fractures of crystalline Precambrian bedrock. The groundwater resources of Quaternary deposits are most important for the public water supply, and therefore it is a part of the critical infrastructure in municipalities. The rural population relies both on local groundwater resources in bedrock but mainly exploits or in small Quaternary deposits by private wells.

Geographical background

Finland is situated between the 60th and 70th northern parallels in the Eurasian continent's coastal zone. The country's geographical position has influenced Finland's climate characteristics, which is in between a transition zone of a continental and maritime climate, and belongs mostly to the boreal zone. Due to the Gulf Stream the mean temperature in Finland is several degrees (as much as 10°C in winter) higher than that of other areas in more continental locations at the same latitude to the east, e.g. Siberia and south Greenland (FMI 2007).

According to Köppen's climate classification, Finland belongs to the temperate coniferous-mixed forest zone with cold, wet winters, where the mean temperature of the warmest month is no lower than 10°C and that of the coldest month no higher than -3°C (FMI 2007, Essenwanger 2001). A typical feature is that the four seasons are distinct, although rainfall is, on average, moderate in all seasons. The climate between the north and south of Finland is different due to the difference in latitude. The annual mean temperature in south Finland ranges

between 3 to 6 °C, while in the north is between -1 and +3 °C. The annual precipitation varies in the central and eastern parts of Finland between 600 and 760 mm, in the western and northern parts of the country it is about 400-650 mm (FMI 2007). Since the evaporation is about 340 mm, the annual water budget is positive in Finland, and groundwater recharges every year.

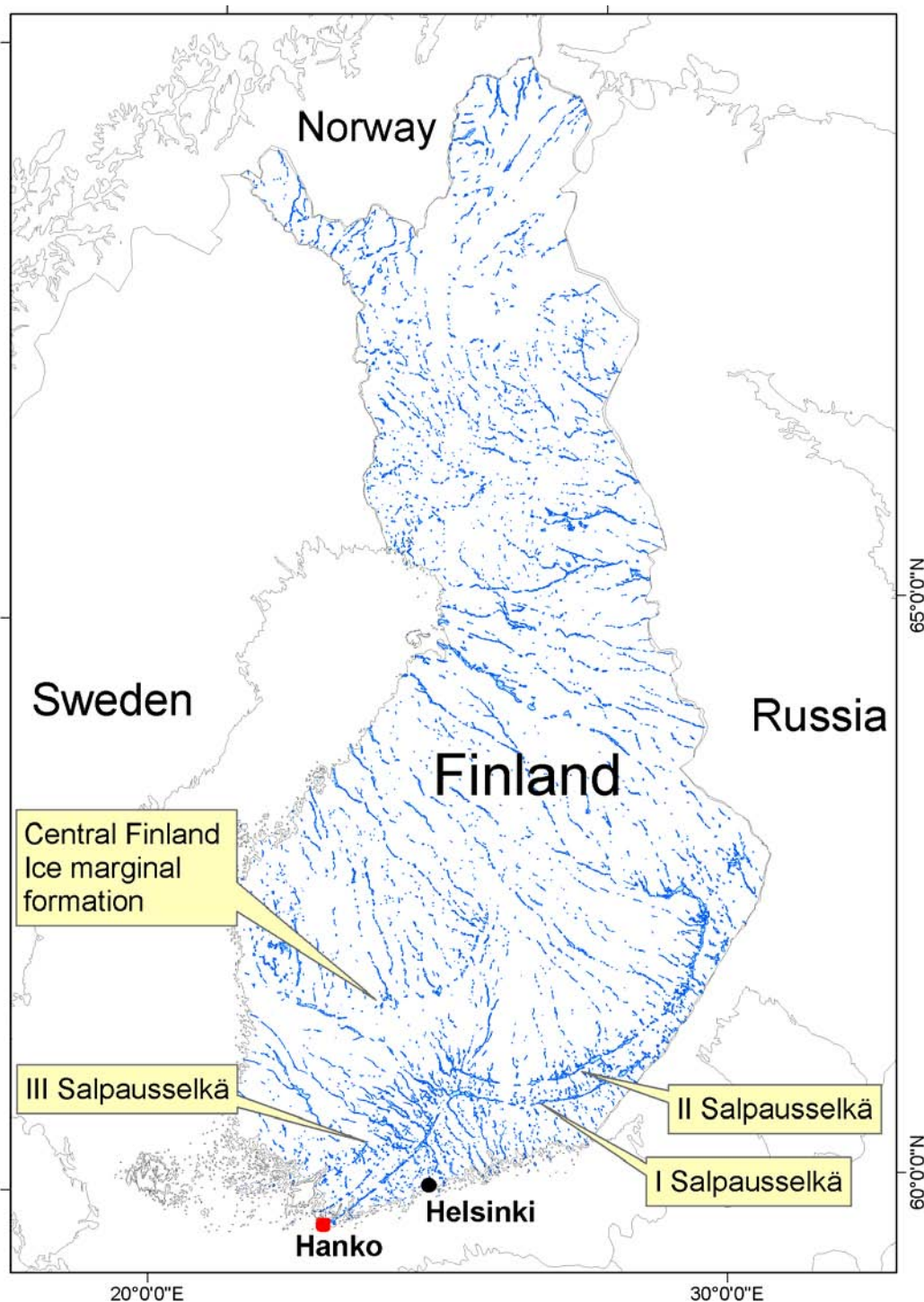


Figure VI—1 Map of quaternary sand and gravel deposits (in blue), the most important shallow groundwater resources in Finland. The three Salpausselkä formations are indicated. (Base map data © National Land Survey of Finland)

The harsh climatic conditions in Finland have created a special attitude to those hazards the climate provides for the infrastructure of water supply. Pipelines are built beneath the level of winter frost, which in south Finland is about 70 cm, and water wells are well-protected against the low temperature.

The old, crystalline bedrock in Finland is part of the Precambrian Fennoscandian craton and consists mainly of Archean and Paleoproterozoic rocks (Lehtinen et al. 2005). The majority of the Quaternary overburden observed today was deposited about 10 000 years ago, during and after the Weichselian glaciation. The contact between bedrock and overburden is very sharp.

Groundwater recharges in Finland in both Quaternary deposits and bedrock fractures. In the coastal area of south Finland the groundwater level reaches its maximum in winter or in early spring (Soveri et al. 2000). During the spring and early summer, the groundwater level decreases to the minimum. The remarkable and useable groundwater resources are from shallow groundwater aquifers, mainly from Quaternary permeable sand and gravel formations. About 7% of the land area in Finland is covered by glaciofluvial deposits (Salonen et al. 2002) (Figure 1). The significant aquifers in south Finland are located in the three Salpausselkä ice-marginal formations and other sand and gravel formations. The First and the Second Salpausselkä run parallel in hundreds of kilometers through the large extensive area from the east to the Hanko area in the south of Finland. The Third Salpausselkä, on the hand, has a smaller size and found deposited only in the western part.

The water table of shallow groundwater is often quite near the surface and therefore easy to exploit. The depths of the water tables vary from less than a metre to more than thirty metres, with an average depth of about 2-5 metres.

Groundwater resources and water supply as part of critical infrastructure

Freshwater is one of the most significant natural resources for life on Earth. Only the well-advised use and protection of freshwater resources might preserve the current level of current life and standard of living in Europe. Water resources and a workable water supply belong to the critical infrastructure in society and need special protection. The most important freshwater resources are located in groundwater aquifers. In these formations, the water is well protected, better than surface water, but even this water is at risk. The potential risks might be natural or man made. The water supply system by itself is sensitive and vulnerable for climatic, economic, technological or political risks and needs special protection.

Freshwater provides drinking water and household water to communities and households and supports irrigation for farm production. Many industry processes and productions need plenty of water of good quality. Approximately 0.7 million cubic metres of groundwater per day are abstracted from the aquifers in Finland (SYKE 2007). Groundwater (including the artificial recharge groundwater) from glaciofluvial aquifers of sand and gravel formations contribute about 60 % of public water supply, and the number is expected to increase up to 75 % in 2010 (Figure 2). The public water system serves about 4.7 million inhabitants in Finland, about 0.5 million inhabitants in rural areas depend on local groundwater resources and use private wells. The number of water works with more than 50 users, was 1900 in Finland in 2001. The calculation of water consumption per

inhabitant was then 240 L/d, including the industry. About 60 % of the groundwater consumption is approximated as household use (SYKE 2007). The average price of raw water and use payment was 2.30 EUR/m³ in 2001. The approximated price for water for one person per month was approximately 13 EUR. This figure excluded the payments of basic charge and payments of instruments, which vary in different municipalities. The water system pipeline network in Finland comprises of 83,614 km, of which plastic pipes amount to 72,206 km, iron pipes 8,382 km and pipes of other materials 3,026 km (SYKE 2007).

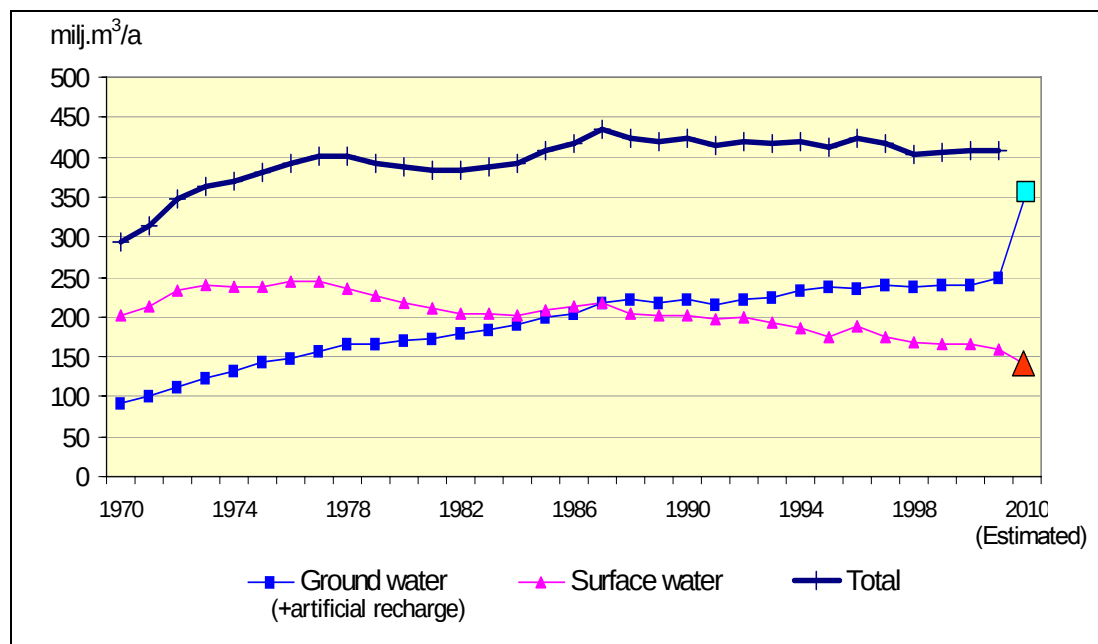


Figure VI—2 Amount of water distributed by public water works in Finland during years 1970 – 2001 (milj.m³/a). (Modified from SYKE 2007)

Groundwater quality in its natural state is usually of high quality in Finland. Finnish groundwater is generally of the Ca-HCO₃ type, which is typical for glaciated areas, with low concentrations of electrolytes, and low pH, alkalinity, calcium and magnesium. Occasionally, especially in spring time the KMnO₄ numbers are high and aluminium and iron values are increased (Lahermo et al. 1999, Backman 2004). Groundwater quality depends on geological, anthropogenic, climatic, and marine factors. In some areas the groundwater can contain high concentrations of harmful elements such as nickel, manganese, arsenic, fluorine or radon of geological origin. Human activities in some agricultural areas lead to an increase in nitrate and potassium concentrations and de-icing of roads causes contamination in some aquifers. However, groundwater reserves in Finland do not normally suffer from contamination on a wider scale, because individual bodies of groundwater tend to be small. The risk of contamination is highest in areas where soils consist of high permeable layers of sands and gravel, which can be easily infiltrated by pollutants.

Groundwater resources along the coastal area are at risk, not only due to the change of hydrologic patterns. They also are vulnerable to sea level rise, especially in coastal areas along the southern coast, where future sea level rise is expected to

be higher than along the west coast. In Finland, approximately 600 aquifers of total 12,982 aquifers (Britschgi and Gustafsson 1996) extend to the seacoast (Figure 1) and there are lot of public water works and private dug wells in these aquifers. In addition, there are numerous summer cottages on the coast and by tradition each cottage has its own well.

Previous studies

The morphology and sedimentary of the First Salpausselkä formation and the groundwater aquifer in the Hanko area have been investigated by many studies (e.g. Fyfe 1991, Kielosto et al. 1996). The first plan for groundwater protection for Hanko was conducted by Harju (1997), and the plan was updated by Maa ja Vesi (2005). The Geological Survey of Finland (GTK) studied the geological structure of groundwater aquifer in the Hanko and nearby areas (Breilin, et al. 2004). The study clarified the geological structure of bedrock and simplified the groundwater model of the First Salpausselkä formation – the main groundwater aquifer formation. The accommodation between groundwater protection and aggregate supply, also known as the POSKI project, was carried out in the provinces of Uusimaa and Itä-Uusimaa 1998 – 2004 (Kinnunen et al. 2006). The project aimed at protecting the environmental values of the geological formations as well as securing the supply of high quality ground water for the communities and high quality aggregate for building purposes. A detailed geological modelling of the sedimentary and groundwater area was carried out in a small oil contamination area in Trollberget (DEMO-MNA, Jørgensen et al. 2006), 5 km north of Hanko town centre, together with the feasibility study of a remediation technique for oil and heavily contaminated soils, which is located in the northern part of the Hanko groundwater aquifer. The above studies showed that the sedimentary and morphology of the First Salpausselkä formation is quite complicated with alterations of gravel and sand layers and layers of fine sediments such as silt and clay. Groundwater levels also vary and many places are located very close to the surface, which are vulnerable to contamination.

The potential impacts of climate change on shallow aquifers in coastal regions range mainly from changes in precipitation patterns, in evaporation, and subsequently change in groundwater recharge, and finally seawater intrusion to the aquifer. These subjects have been examined in two Baltic Sea Region (BSR) INTERREG IIIB projects, “Sea level change affecting spatial development in the Baltic Sea Region” (Schmidt-Thomé 2006a and Schmidt-Thomé 2006b) and “Developing policies & adaptation strategies to climate change in the Baltic Sea Region (ASTRA)” (ASTRA 2007), both coordinated by the Geological Survey of Finland (GTK). The project groups consisted of cities and municipalities that closely cooperated with several European research institutes. The recent statements of the Fourth Assessment report issued by the Intergovernmental Panel on Climate Change (IPCC 2007) state that climate change is no longer avoidable, underlined the importance of such projects. Meanwhile the SEAREG project focussed mainly on sea level changes and following potential impacts on changing flood prone areas, the follow-up project, ASTRA, aims at developing regional concepts to cope with a wider range of potentially adverse effects of climate change, e.g. droughts. Although climate change is a global problem, its impacts will vary locally and therefore it is a challenge to develop adequate adaptation

strategies. The awareness that adaptation strategies evolve from regional experience and that their integration is better feasible and judge able at the regional rather than at the global level, was a further motivation for ASTRA. Much the same subject matter was discussed in the FINADAPT-project (Silander et al. 2006). The results of these previous projects are here applied on a new case study area, including a wider scope, i.e. risks.

Concerning the associated hazards of climate change, the major endeavour for humankind is to provide safe limits for both nature and humanity. The global population and economy will grow further. Most energy and industrial production, as well as transportation, will rely on fossil fuels also in the near future, and climate change scenarios indicate an increase in the average global temperature of up to 6.4 °C by 2100 (IPCC 2007). Therefore regional consequences, in particular with respect to future planning strategies, must be evaluated carefully.

Climate change in the BSR

The SEAREG project developed three scenarios ranging from 'low case' to 'high case' for winter mean sea surface height for 2071-2100 using a reference data from 1961-1990. In the Hanko area, the low case scenario indicates a drop of the 1990 sea level by -35 cm, the ensemble average scenario 15 cm and the high case scenario of 64 cm sea level rise, respectively (Meier et al. 2004 and Meier et al. 2006). Although mean annual sea surface height is an important figure, storm surges pose a greater acute risk in the Baltic Sea Region (BSR). For example, the westerly winds of 9 January 2005 caused the sea level to rise 151 cm in Helsinki and 130 cm in Hanko. The storm surges that push the water masses towards the south coast of Finland are reckoned to become more common in late 21st century (Marttila et al. 2005).

Scenario simulations have shown that for the BSR some serious consequences of climate change can be anticipated by 2100. This holds for warming and changes in precipitation patterns, as well as for sea-level increases. Recent state of the art knowledge implies that effects like temperature increase and sea-level rise have been underestimated over recent decades. If the prognosis of the IPCC (2007) comes true, and if humankind does not take appropriate action to reduce atmospheric carbon dioxide concentration radically, this would lead to the warmest period on Earth in 1,000 years, and probably even the last 100,000 years. This large-scale warming is expected to be accompanied by increased frequency and/or intensity of extreme events, such as heat waves, heavy rainfall, storms and coastal flooding. Model results and examination of measured data in several regions show that there might be strong variations in precipitation patterns. Changes in temperature extremes have already been observed, for example during the summer of 2003, with maximum heat record of 33.3 °C in the Mietoinen province, southwestern Finland. Model outputs show changes in extreme events for future climates, including increases in extreme high temperatures, decreases in extreme low temperatures, and increases in intense precipitation events.

An important threat for BSR is the rise in sea level. Although the SEAREG project has already attempted to estimate future risks, new results imply that the rise in sea level is accelerating. For example, neither the rapid melting of the Greenland glaciers over the last 20 years, nor the measured and simulated gauge levels, was considered adequately. Also, it is highly likely that an increase in

precipitation will occur in the Nordic countries (IPCC 2007). Even though an increase in precipitation might sound like good news, the change in the precipitation pattern has to be taken into account too. It is most probable that the precipitation maximum will shift towards the winter months and that drier summers can be expected (Figure 3). This might lead to summer droughts, which have already been experienced in the BSR, the latest being in 2006. Overall the Fourth Assessment Report shows that the performance of the climate change models was significantly improved and there is no longer any doubt that human activities force of these serious developments.

For the BSR, this also implies that the threat of climate change impacts cannot be neglected any longer. Climate change should therefore be included in any risk assessment for future territorial development.

Based on the results of the SEAREG and ASTRA projects, the effects of climate change that mostly concern cities and municipalities are sea level change and flooding. The drought problem, also for Nordic states, has not yet been widely understood as a real challenge. Territorial development, including spatial planning, is identified as playing a key role in climate change adaptation, and therefore it is future land use in particular that should be addressed by climate change studies (Schmidt-Thomé 2006b).

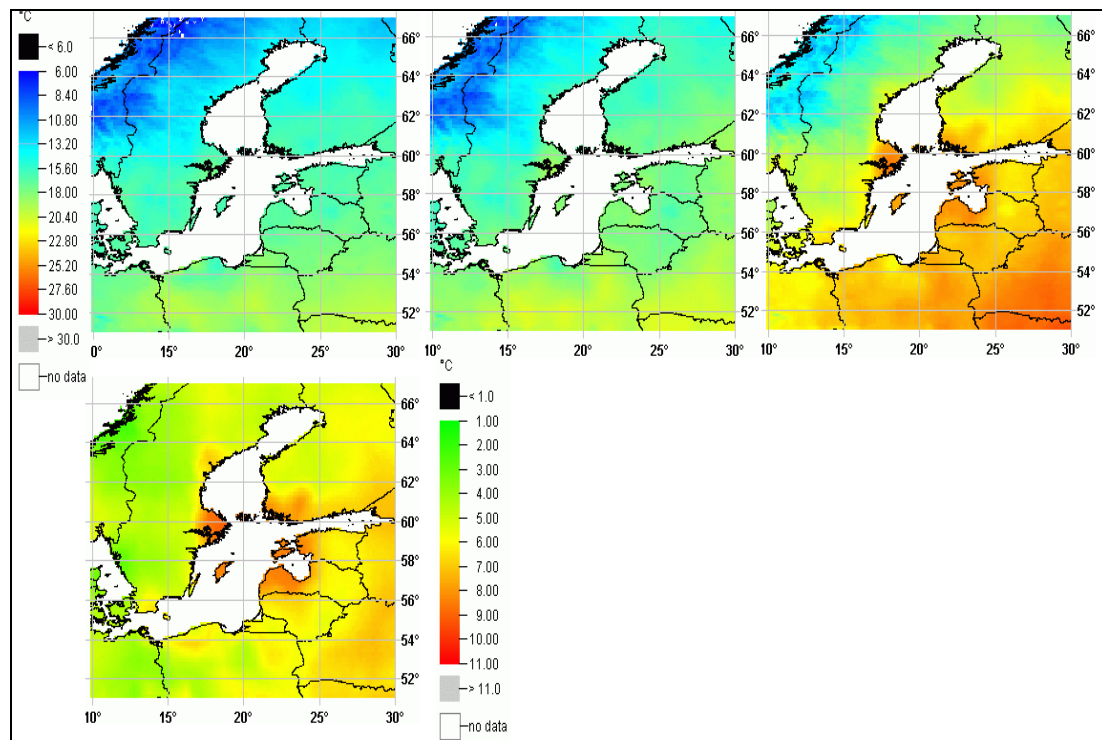


Figure VI—3 Mean temperatures for the summer seasons (June, July, and August) for 2001, 2050 and 2099 (upper panel) and the difference 2099/2001 (lower left panel). (Potsdam Institute for Climate Impact Research, based on CRU/ATEAM data; Kropp 2007).

Aim of the study

The objective of this study is to provide an overview of the potential risks of the shallow groundwater resources and water supply from both human activity and

climate change, including risk management in one coast area aquifer. The results obtained from this case study can be applied to other similar aquifers, as it outlines possible threats that would impact shallow groundwater resources, considering the implications for the management of water resources in different sectors. On the other words, on the basis of this one case study it was possible to create a model of potential risks for groundwater and water supply at this aquifer.

The selected case study area was a large sand and gravel formation at Hanko peninsula, Hanko aquifer, in the Southwestern coast of Finland. The Hanko aquifer was chosen because the permeable sand and gravel layers of this aquifer extends until the seashore, the water of the aquifer is in public use, and there are lots of human activities in the area. In addition, the hydrogeology of the area had already been studied intensively, so that much data was available. Also, the Hanko Town Water Work was a very cooperative partner. There are several of comparable aquifers in Finland, in Sweden and in other countries on the coastline of Baltic Sea, so that the results may be easily adapted to other areas.

The potential effects of climate change on the Hanko shallow groundwater resources and infrastructures would cause risks not only from the change of precipitation and warmer temperature, but also from the rise of sea water level, making the coastal aquifers more vulnerable to this change than the aquifers in the main land. The study also describes how the infrastructure and management of Hanko Water might economically adapt and respond to changes in climate, in context of higher future population and change in land use and technology.

Shallow groundwater resources have been studied extensively in Finland, and some local groundwater risk assessment has been done, but the study of effects of climate change on coastal aquifers is a new point of view. The discussion of all these factors together in relation to a coastal aquifer is also new.

6.2 METHODOLOGY AND MATERIALS

Method and materials

The study method was to produce knowledge about risk assessment and risk management concerning groundwater in one coastal aquifer. The results provided from this case study area can be applied to other similar aquifers. Some information was collected from previous studies and a part produced by this current study.

All available data from Hanko aquifer was collected. Data was mainly collected from the Geological Survey of Finland, the Hanko Town Water Works, the Uusimaa Regional Environment Centre, and the Finnish Institute of Marine Research (FIMR).

The most empirical and original part of the material, the groundwater level monitoring data of the Hanko aquifer, was produced by GTK between 12 February 2007 and 12 June 2007 in two observation wells owned by Hanko Town: HP306 observation well in the north-west side and HP66 observation well in the south-east side of the aquifer. The locations of the observation wells are shown in Figure 5. The observation well HP306 is located in the Hopeasanta beach, about 100 m from the coast and about 100 m from the Hanko Town main water works. The

observation well HP66 is located on the south beach, about 215 m from the Mannerheimintie water works and 50 m from the coast.

The measurement was done using the VanEssen Diver and VanEssen Barometer tools (Figure 4). Pressure and temperature were measured in every 30 minutes in both diver sensor and in air pressure sensors, which were situated in the housing of the HP66 observation well. The groundwater level was calculated from the pressure in a diver sensor and was compensated with air pressure. Sea level monitoring data of the same period were received from the Finnish Institute of Marine Research. This data was measured every hour.

The most important factors controlling the sea level in the Baltic Sea are air pressure, wind, water flow through the Danish Straits, and ice conditions in winter. According to FIMR (2007), tide has an effect of only a few centimetres on the Finnish coast. The currents flow through the Danish Straits, caused by sea level differences between the Baltic Sea and the North Sea, and can cause a change in the total amount of water in the Baltic Sea (bathtub effect). The air pressure is one of the main factors that affect the sea level. An air pressure change of 1 mbar corresponds to a sea level change of 1 cm. The normal pressure variations may thus cause a sea level variation of several tens of centimetres.



Figure VI—4 Groundwater monitoring tool installation at the well HP0306. (Photo by S. Luoma)

6.3 HANKO AQUIFER

Hanko study area

The topography of the Hanko Peninsula is relatively low and the average altitude is only about 13 m a.s.l. (N₆₀) (Figure 5). The studied 14 km² sand and gravel area, the Hanko aquifer, is a part of the First Salpausselkä end moraine and the altitude in the area of this formation is about 10 – 12 m increasing slowly towards northeast. The general feature of the aquifer is flat plain shelving to the seaside on its south and northwestern side.

The study area belongs to the town of Hanko, which lies partly on top of the aquifer under study. Hanko has about 10 000 inhabitants and an area of about 800 km². The economy consists of 60 % services and 38 % industry. The town has a busy port, mainly handling transit trade to Russia, and many chemical industries.

Hanko is also a popular summer resort with a coastline of some 130 km, of which 30 km are sandy beaches.

Geological and hydrogeological background

The shallow groundwater aquifer of the Hanko coastal area belongs entirely to the First Salpausselkä formation (Figure 5). The primary sand and gravel formation deposited in the front of the ice sheet into deep water in the end of the Weichselian glaciation in time span of 200 years, 11 250 – 9 900 years ago (Fyfe 1991, Saarnisto and Saarinen 2001). The form of this primary sand and gravel formation was quite narrow and low (Fyfe 1991). When the ice sheet withdrew from the area, this deep water sitting formation was covered by fine sediments - fine sand and clay layers - of Ancylus Lake and the Littorina Sea. The sea level has been regressive since the glacial period, caused by the isostatic land uplift - the only exception to this was the transgression of Ancylus Lake and the Littorina Sea, when the sea level rose for a while (Kielosto et al. 1996).

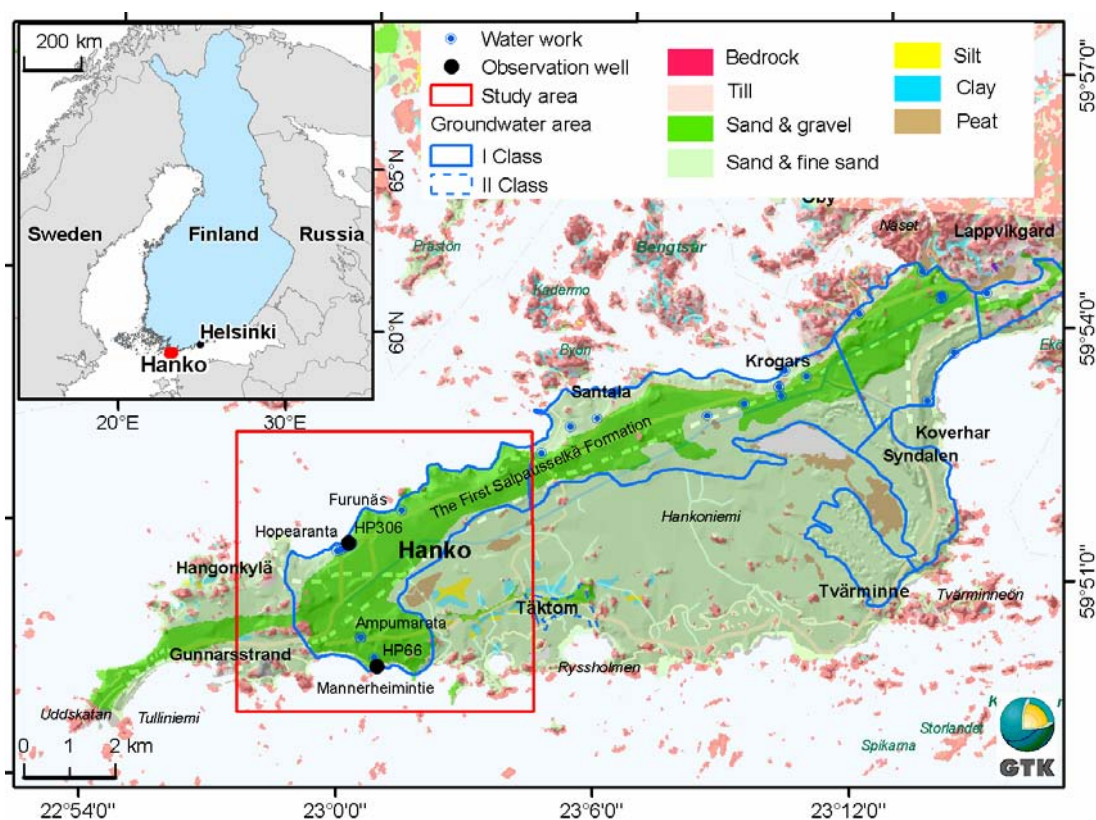


Figure VI—5 The Hanko case study area on the Quaternary deposit map.¹¹⁵

After the area emerged, the Salpausselkä formation was exposed to sea waves and wind. Therefore littoral sand deposits and fine sand wind deposits covered the clay and fine sand sediments in places. The bedrock in the Hanko area consists mainly of Precambrian crystalline igneous and metamorphic rock, strongly fractured along

¹¹⁵ Quaternary mapping data © Geological Survey of Finland; Base map data © National Land Survey of Finland.

preferential directions. The bedrock is mainly covered by Quaternary deposits, with only a few outcrops in the area.

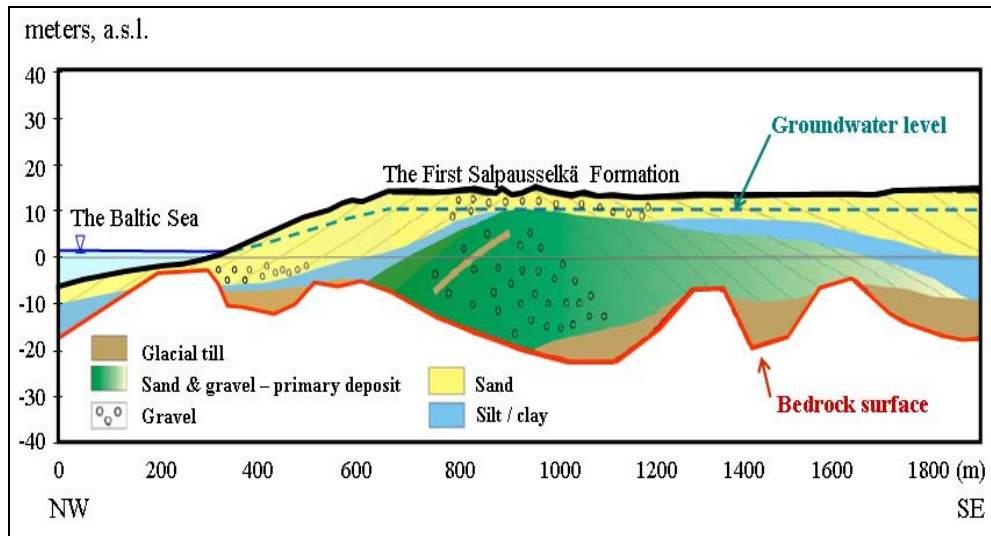


Figure VI—6 Conceptual geological model of the First Salpausselkä Formation in the Hanko main groundwater area. (Modified from Breilin et al. 2004)

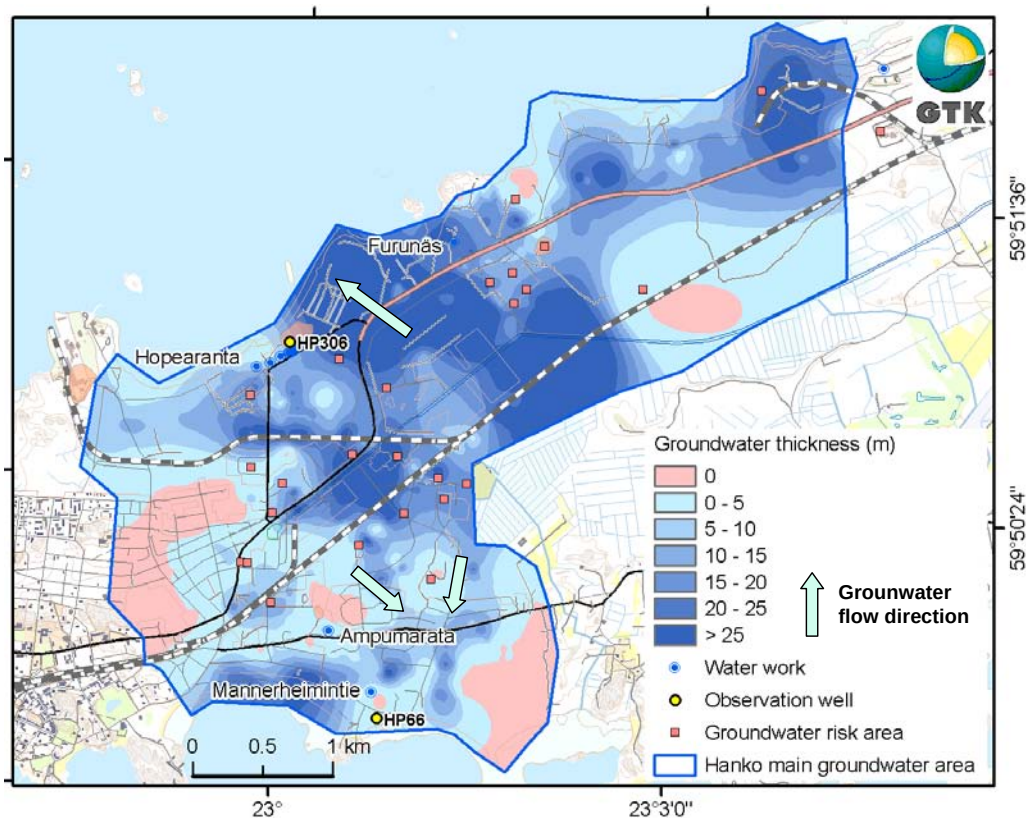


Figure VI—7 Groundwater thickness in Hanko main groundwater area. The thickness of groundwater reflects the surface of the bedrock under the Quaternary deposits. (Modified from Breilin et al. 2004)

The complicated geological structure of the First Salpausselkä formation results in complicated groundwater conditions. Permeability varies in the Hanko aquifer due to the changes in the grain size and thickness of the different layers. The structure of the aquifer in the northwest part is quite different to the southeast part.

According to drillings, the sand and gravel layers are varying with clay and silt layers (Figure 6). In many places the geological stratigraphy from ground level downwards is: first sand and gravel layers with good water conductivity, then silt and clay layers with weak conductivity, followed by sand and gravel layers with good conductivity. According to Breilin et al. (2004) the groundwater level in the study area varies from less than 2 meters to more than 15 meters below surface. The groundwater table is at its deepest level in two different parts in the northern and southern part of the formation (Figure 7). Right by the Baltic Sea coast the groundwater table is near the ground surface. Generally, the groundwater table is less than + 2 m a.s.l. (N₆₀), only in the centre part of the formation the groundwater table is + 4 - +6 m a.s.l. (N₆₀).

Water supply

There are four separate public groundwater works in the studied aquifer (Figure 7). In 2003, the total water use of the town of Hanko was on average 4 630 m³/d. The combined pumping volume from four water works in the study area was 1 430 m³/d, which contributed about 30 % of the Hanko's water production, even though the yield and the capacity of this formation are much larger than that now used.

The name of the oldest water works is Hopearanta in the north part of the formation, built in 1907. This is one of the oldest water works in Finland. The pumping rate of this water work is of 700 – 800 m³/d. The water work consists of three different wells and the total pumping permission is 1 200 m³/d. The recently defined catchment for the wells is about 1 km².

The water works of Mannerheimintie is located in the south part of the aquifer quite near the town. The pumping permission is 720 m³/d and the daily use in general is about 320 m³/d. However, at the moment this water work is not in use. The current estimation of the size of the catchment is about 0.5 km².

The water work of Ampumarata has a pumping permission of 2200 m³/d, but it is not possible to get that much water from the two wells in the area. The water quality is not good enough in this water works, the problem being too high iron and manganese contents. The water use is now only for the irrigation of the sports area.

The water works of Furunäs has been closed since 1982 because of a leakage from the sewer water system of a nearby pharmaceutical factory.

In addition to the water works, there are some private wells in use, mainly for irrigation. There are also many groundwater observation wells, mainly in the vicinity of the water works but also elsewhere in the area of the aquifer. The length of underground water work system network in Hanko is in total 155 km.

Groundwater quality

The Hanko aquifer has been burdened by different activities and factors, and the water quality has decreased in places. The water quality at the groundwater works is regularly sampled by the health authorities and the staff of water works. The analyses and measurements are according to the Act of Water quality requirements

for water works (Sosiaali- ja terveystieteiden ministeriö 2000). The water levels in the vicinity of the groundwater works are also regularly monitored.

In general, the water quality at the Hanko water works is good. In Hopearanta the chloride content occasionally increased, but the values were, however, less than the limit value. The reasons for the chlorine-increased values may be seawater intrusion, relic salt water, de-icing of the road or the landfill. Also, the iron and manganese contents increased in some samples. Ampumaranta water works has had problems with high iron and manganese concentrations, and there was an observed increase in volatile organic compounds (VOC) and small amounts of pesticides. The fluoride content has also increased occasionally at the Ampumaranta and Mannerheimintie water works.

Table VI—1 Comparison of groundwater quality parameters in the Hanko peninsula to Finnish average.

Parameter	Shallow groundwater in Hanko peninsula *		Shallow groundwater in Finland**	
	Median	Mean	Median	Mean
pH	6.7	6.7	6.4	6.5
El. conductivity, mS/m, 25°C	13.4	18.48	12.5	16.4
Chloride, Cl ⁻ , mg/L	10.5	19.08	4.46	8.6
Sulphate, SO ₄ ²⁻ , mg/L	15.0	16.79	10.4	14.6
HCO ₃ ⁻ , mg/L	41.5	44.69	32.9	51.9
NO ₃ ⁻ , mg/L	0.6	1.58	3.19	8.43
Ca, mg/L	11.9	17.2	11.4	15.2
Mg, mg/L	1.68	2.68	2.38	3.83
Na, mg/L	6.71	12.75	4.18	7.02
K, mg/L	2.02	2.33	2.78	4.97
KMnO ₄ -number, mg/L	3.4	15.43	4.5	8.48
Fe, mg/L	0.03	0.17	<0.03	
Mn, µg/L	9.23	12.58	4.36	59.1
Al, µg/L	9.84	46.1	18.5	101
Ba, µg/L	5.76	6.56	18.1	28.0
Number of samples	23	23	739	739
* GTK groundwater database 4.2007				
** Lahermo et al. 1999				

The database of GTK includes 26 groundwater samples from the Hanko peninsula. Twenty-three of them are from shallow groundwater and three from hard rock groundwater (GTK groundwater database 4.2007). The interest focuses now, however, to the shallow groundwater. Five of these samples are located in the area of the studied Hanko aquifer. The electrical conductivity values are on average a little higher in the groundwater of the Hanko peninsula compared to the rest of the country (Table 1). The higher values depend mainly on the higher chloride and sodium values in groundwater, which is typical for seacoast areas: the sea salt affect as aerosols on the concentrations of precipitation and therefore also on groundwater concentrations. Also, sulphate and bicarbonate values are on average a little higher, but nitrate, manganese and potassium values are lower in the groundwater of the Hanko peninsula than in rest of Finland. Concerning trace and heavy metal concentrations, the manganese values are higher, and aluminium and barium values are lower in Hanko than in the rest of the country. The solubility of aluminium is heavily depending on the pH values. Manganese and iron values are

often higher in the coastal area than in inland (Lahermo et al. 1999). Concerning other studied water quality parameters, the concentration levels of Hanko are comparable to the rest of Finland.

Fluctuation of groundwater level

The fluctuation of the groundwater levels from two observation wells, the sea level and the atmospheric pressure during the monitoring period is presented in Figure 8. During the monitoring period, the sea level varied between -0.43 m and +0.57 m (N₆₀), which corresponded respectively to the period of highest and lowest air pressures. On the other hand, the results indicated that variations of sea levels affected the groundwater level directly. During the sea level rise, the pressure from sea level rise pushed the groundwater level high up as well. Groundwater levels in the observation wells varied between +0.064 m and +0.762 m (HP66) and between -0.153 m and +0.24 m (HP306). The differences of changes in water levels of those two observation wells probably suggest the difference in hydrogeological properties in different parts of the aquifer. The permeable layers in the Mannerheimintie area (HP66) are thinner and the size of the reservoir is smaller than in the area of Hopearanta (HP306). In addition, the pumping of the Mannerheimintie water works was not in service during the monitoring period. Groundwater levels in the HP306 observation well were very close to the sea level and in many intervals during the sea level rise; groundwater levels from this well were even below the sea level. HP306 is located close to the main water work wells – three separated wells - and is affected by the water drawdown. The pumping from the wells to the water tower is continuously about 600 – 900 m³/d. The pumping was less for only some hours during the night.

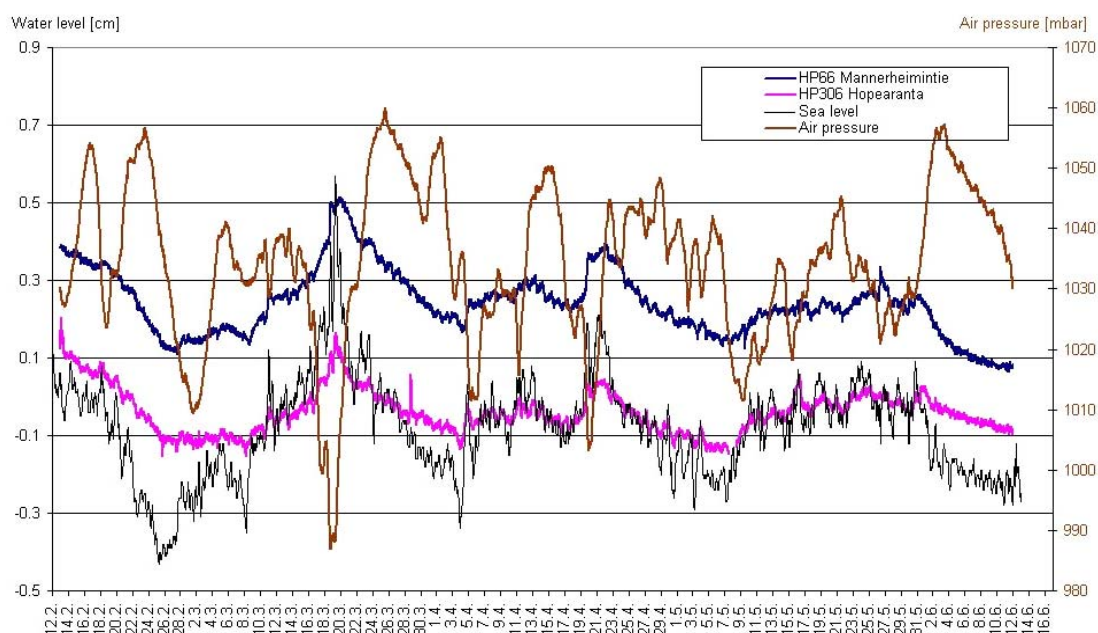


Figure VI—8 Groundwater level of observation well HP66 (in dark blue) and of observation well HP306 (in red), sea level (in black) and air pressure (in brown) data during 12.2 – 12.6.2007.

This observed data shows that the sea level changes have a direct, remarkable and very fast effect on the groundwater level. The time lag between the seawater rise and groundwater level rise seems to be only a few hours in this highly permeable aquifer. Thus, based on this data and according to the climate change scenarios, it can be concluded that the significant rise of sea level in the Hanko coastal area could cause problems to the water supply managements and infrastructure planning in the Hanko and in many other coast aquifer areas.

6.4 RISK ASSESSMENT IN THE HANKO AREA

Threats to shallow groundwater aquifer and water supply

Threats to the Hanko shallow groundwater aquifer and water supply are below classified into two main categories: (1) threats from human activities and (2) threats from climate change. The groundwater based water supply is part of the most important critical infrastructures (e.g. distribution network, pipe network), because shallow groundwater is the main water source available, with easy abstraction methods, and the communities and industries in the Hanko area rely on it for both domestic consumption and industrial use.

Risks, either anthropogenic or natural, can affect groundwater quantity or quality. Often, the changes in groundwater quantity – increase or decrease of groundwater table – affect changes in groundwater quality.

Basically, it is a good situation if the amount of groundwater increases, but this can affect significantly the groundwater quality. The infiltration time will be shorter, and that means that the water will not be purified well before it reaches the groundwater table. During the infiltration the quality of the water improves; the unsaturated zone works like a refiner by different geochemical processes. If the span of water in this zone is too short, all the geochemical processes have only a short time to complete and such things as the risk of groundwater contamination by microbes will increase. The hydrogeological processes in the unsaturated zone are not yet well known in Finland. The corrosion of different materials in buildings and constructions will increase if the groundwater table varies greatly.

If the water table decreases, the most remarkable result is that wells may no longer reach the groundwater when the water quantity diminishes. Sometimes, it is possible to dig deeper wells, but small aquifers may dry up.

The rise in sea level rise has the long-term high potential risk of the intrusion of seawater, which would increase the corrosion of the water pipe system, resulting in high operation costs and possibly groundwater contamination. Capital costs of infrastructure, such as the rebuilding of wells and water pipe line networks or water treatment of contaminated groundwater would increase. In addition, the rise of the sea level will push the groundwater level up and in long term, it could cause reductions of infiltration interval of water because of thinner infiltration zone. The thinner infiltration zone could worsen the groundwater quality, especially in the area of high permeable sand and gravel zones.

All the changes in groundwater circumstances may, however, have economic effects, for example due to the necessities of rebuilding wells or pipelines or by

water treatment. Water transport from other groundwater resources might be a possible alternative, but this is very costly.

Human threats to groundwater and water supply

The human (or technological) threats to groundwater currently under discussion may be events that happen once or they may be continuous. The settlement of Hanko on the area of the Hanko aquifer is mainly a threat not only to groundwater quality but also to its quantity. The Hanko shallow groundwater's risk areas are shown in Figure 9.

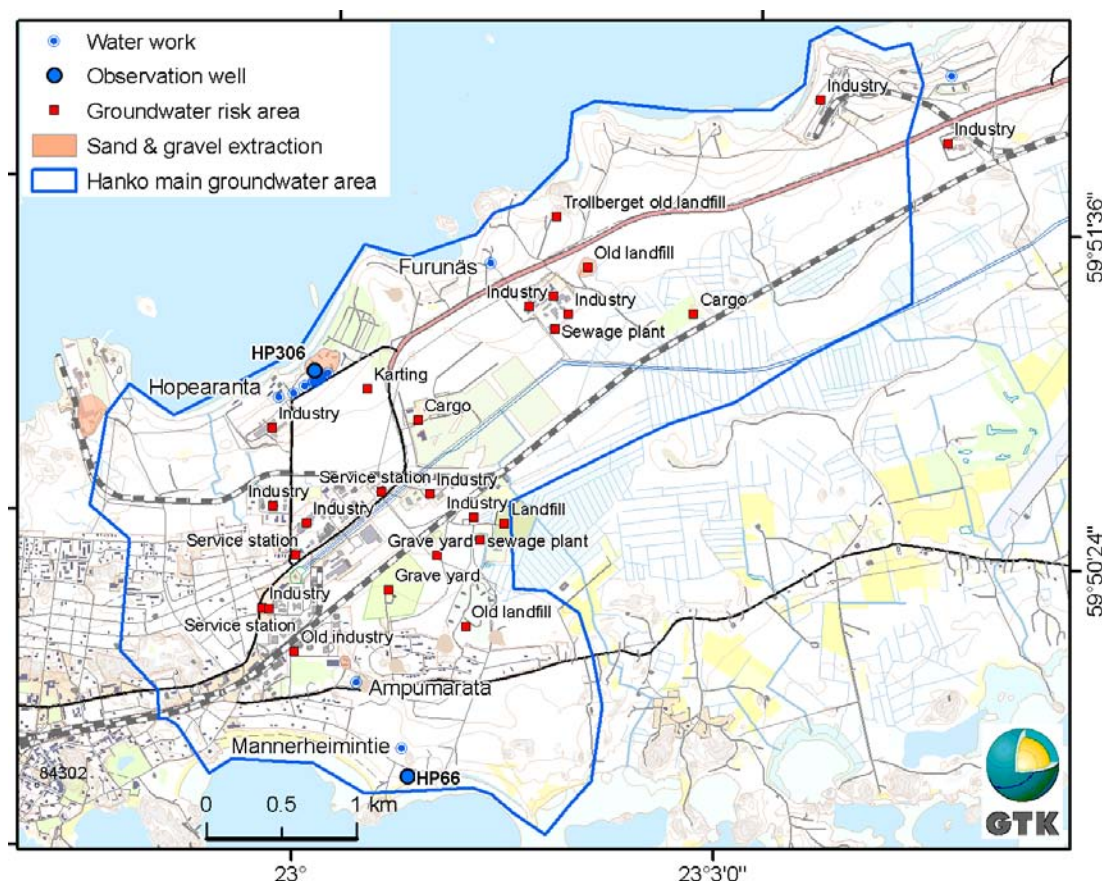


Figure VI—9 Map of Hanko groundwater risks. (Modified from Maa ja Vesi 2005)

While the groundwater aquifers and water supply are vulnerable to terrorism and sabotage, either directly or through infrastructure interdependencies, the main direct risks seem to be of less dramatic nature of human activity. Hanko is an important harbour and industrial town. It is highly industrialized and there are number of factories of small and medium sizes located in many parts of the Hanko shallow groundwater aquifer area.

The area of Hanko Town has an underground sewer system network of 139 km, with 25 pumping stations. The condition of the network has in places become weak. The oldest part of the sewer system as built in the 1910s. The material in this old sewer system is cement. The sewer system network is located beneath ground and above the groundwater table. During heavy rain, the rainwater may

reach the sewer system network and cause an overflow. Electrical power failure may also cause an overflow of the sewers when the pumping is interrupted. The span of power failures has since Hanko sold the public power works to a private company.

Problems in the availability of electricity in general are one of the most critical threats in the Hanko water supply, because electricity is the main power supply used for the groundwater pumping and distribution processes.

According to the investigation by Hanko Town the amount of oil tanks in the area of the Hanko aquifer was 403 in 1996 (Maa ja Vesi 2005), of which more than 50% stored underground. Most part (70%) of these tanks had a capacity of more than 3000 L. The oldest tanks are from the 1950's and 1960's and the condition of the tanks is not always known. The responsibility of the good condition of the oil tanks belongs to the owner of a property.

Traffic and transport is a clear threat to groundwater. Highway 25 runs through the centre of the shallow groundwater area. This is the main transportation route that links Hanko to Finnish road network. Transport of dangerous products on highway 25 has increased a lot during last years. The amount of transported dangerous products per one week was 100 – 500 ton in 1992 and 500 – 1 500 ton in 2002 (Maa ja Vesi 2005). The most significant product transfer is the transportation of cars from Hanko to other parts of Finland and mainly to Russia. The Port of Hanko has specialised in car transit and in 2005 the customs of Hanko cleared 43,206 trucks carrying altogether 253,634 cars to Russia from 330,000 cars that were transited to Finland (Finnish Customs 2005). In 2006 the number of cars transited to Finland was up to 530,000 and over two thirds of these cars were transited via the Port of Hanko (Finnish Customs 2006). Hanko has pledged to ensure an ice-free road throughout the winter and spring time. The use of salt for de-icing the main roads has a high potential for intrusion of Na-Cl- salt to the groundwater by snow melting in spring time. Also, the high chlorine content in the water and soil potentially enhance the corrosion of pipelines.

The human threats influencing groundwater quantity is asphaltting of the surface of the Hanko aquifer. Increasing area of the Hanko aquifer has been covered by asphalt. There is a big storage area in the catchment area of Hopearanta water work for the cars transported to Russia. Now a requirement for asphaltting of this area has been claimed. Huge car parks for these vehicles already exist in the area of the aquifer. The asphalt cover on the aquifer surface decrease the infiltration of precipitation and snowmelt water and causes decrease of groundwater level.

In the area of Hanko aquifer are two service stations for cars. One has been located in the east part of the aquifer since the 1960s. The environmental permit for this station was licensed in 2002 (a permit needed for activities that will or may cause environmental pollution or degradation allowed by an environmental authority). The distance from the service station to the groundwater work of Ampumaranta is 700m and to groundwater work of Mannerheimintie about 1200 m. The other service station is located in the vicinity of the groundwater work of Hopearanta, and the distance is about 800m, with an environmental permit licensed at 2003. In addition there was an old, at present closed, service station in the vicinity of Hopearanta water work, where an oil spill happened in 1993.

A few oil spills occurred in the beginning of the 1990s at a place located in the vicinity of the Hopearanta water works, of a distance of about 900 m. The groundwater is polluted by oil in the vicinity of the property and observation wells near the groundwater work recorded the concentrations. Remediation activities started in 1996.

The effects on groundwater of gravel extraction are well known in Finland (Hatva et al. 1993). Gravel extraction increases the variation in groundwater quantity and increases the contamination risk of groundwater quantity since the protective soil horizon will be removed. The area of the Hanko aquifer has one active sand and gravel extraction area and three old sand and gravel extraction pits no longer in use. In addition, there are three old landfills and a partly active landfill in the Suursuo area.

Another significant risk is over pumping and saltwater intrusion. In aquifers close to the coastline, freshwater is in contact with seawater. Fresh water tends to flow on top due to its lesser density. Over pumping, which causes lower groundwater level, may lead to the intrusion of saltwater in to the groundwater aquifer system. The diagrams of groundwater flow patterns along the coastline are shown in Figure 10.

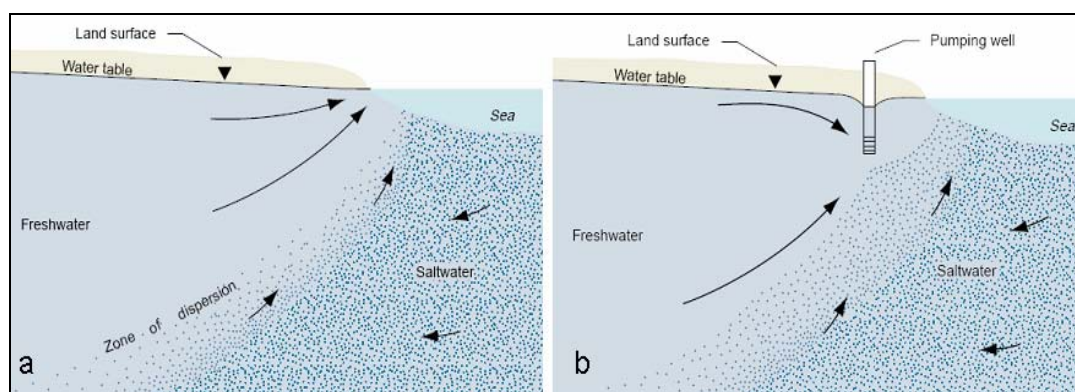


Figure VI—10 a) Groundwater flow patterns and the zone of dispersion in a coastal aquifer, b) Over pumping lowers groundwater level and may lead to saltwater intrusion. (After USGS 2000)

Threats from climate change

The change of climate would alter groundwater both in quantity or quality, mainly through sea level changes as well as changing global temperatures and precipitation patterns.

Sea Level Rise

In the Hanko coastal area, the high case scenario of the study developed by the SEAREG project (Schmid-Thomé 2006a) states that by the end of the 21st century in Hanko coastal area the sea level might rise by 0.64 m. According to the result from the ASTRA project, the Potsdam Institute for Climate Impact Research (PIK) reported that the sea level rise in the BSR would be even higher than stated in the FAR (IPCC 2007) and sea level rise along the Finnish coastline by the end of the 21st century would increase by 0.7 m from the previous scenario of the SEAREG project (Kropp 2007). The Hanko coastal area experienced a maximum sea level

rise of 1.30 m during the storm surge of 09 January 2005 (based on the observations since 1887, (FIMR 2007)). Therefore, by the end of the 21st century the sea level rise in Hanko coastal area could possibly reach approximately 2.64 m in the high case scenario. Figure 11 presents the topographic map of the Hanko coastal area. The areas below a two-metre-contour line are vulnerable to flooding. This may affect not only the aquifers but could also cause some land loss.

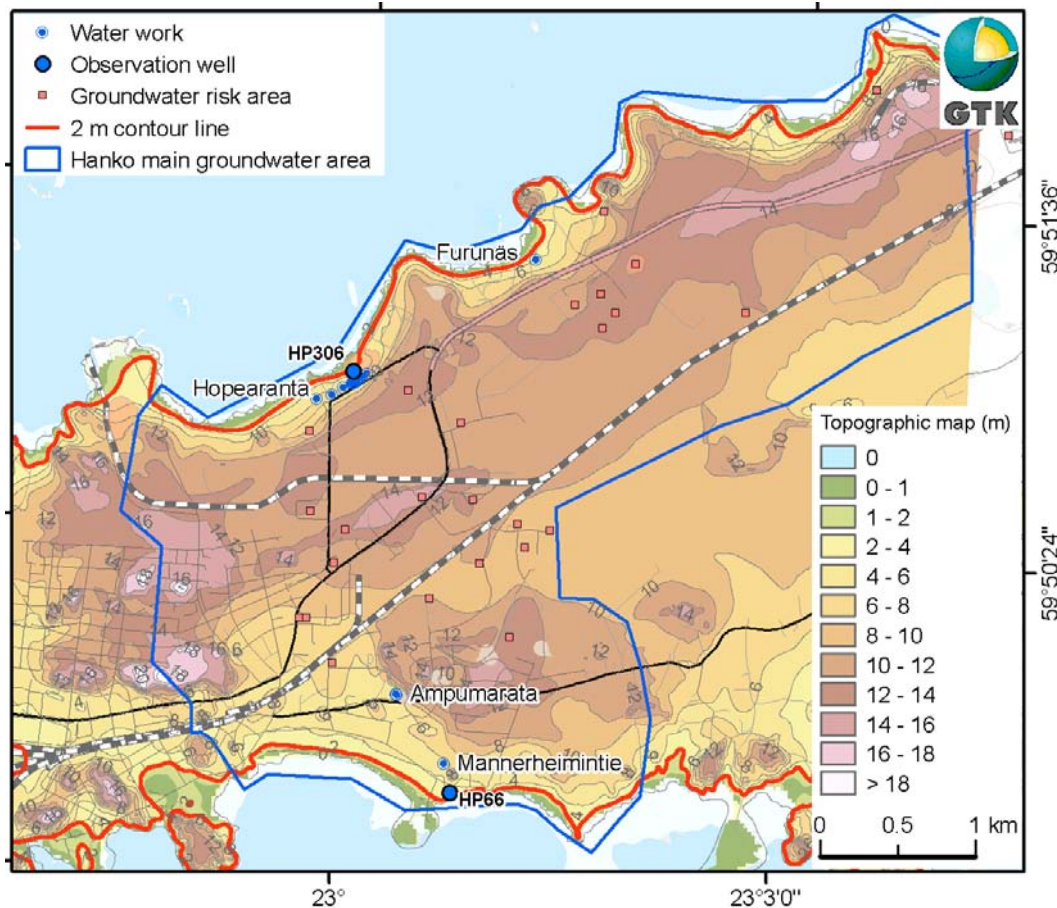


Figure VI—11 Topography map of Hanko main groundwater area with a 2-metre-contour line in red. (Modified from Breilin et al. 2004)

Change of Groundwater Properties Through Changing Temperature

Warmer temperatures would change the pattern of precipitation and evaporation, which would possibly affect the hydrological system, groundwater resources and their management. In south Finland, by the end of the 21st century winter temperatures could increase by as much as 6.5 °C and precipitation might increase by 10-20% (Kropp 2007). Because the recharge of Hanko shallow groundwater is mainly from snowmelts and rainfall, the earlier snowmelts and the longer hot and dry summer could cause higher evaporation and mean less water recharge to the aquifer. This could cause a lower groundwater level, and consequently the reductions of the groundwater budget. On the other hand, increased precipitation (10-20 %) may cause increase of the groundwater table. It is also possible that the changes in precipitation and in temperature and evaporation may compensate each other.

Increases of temperature may activate geochemical processes and increase the rate of the weathering. This would change water quality both in the chemical properties of groundwater, such as higher concentrations of dissolved iron, manganese, metals or trace elements in groundwater, and in its physical properties, such as temperature, colour and solid concentration. In addition, an increase in temperatures could accelerate biological or microbiological processes and increase the potential of contamination of groundwater sources.

In all situations when the groundwater properties or groundwater circumstances will be changed the economic consequences will be high, for instance for building new or deeper wells or water treatment. The widespread use of purification chemicals in water treatment is not good or recommended.

6.5 RISK MANAGEMENT IN THE HANKO AREA

Groundwater protection and management

Legislation concerning the protection of groundwater, the water supply and drinking water quality, is extensive in Finland. Also the legislation, concerning the controlling of these acts is good, but the results in municipal administration are unfortunately limited at present in many municipalities.

The legislation concerning groundwater is mainly arranged by the Environment Protection Act (4.2.2000/86). This relatively new act aggregates all the older acts concerning groundwater and the environmental permit system. The most remarkable content in environment protection act is the Water Act (19.5.1961/264) and there the Land Extraction Act, Land Use and Building Act, Public Health Preservation Act, Waste Act, as well as the Legislation on Prevention of Chemical and Oil Damages. The most important parts in the Water Act are the Groundwater pollution prohibition and Groundwater modification prohibition. These prohibitions are categorical and guide activities in areas that are important concerning groundwater.

In Finland, the health authorities control the quality of groundwater used as household water. Water quality requirements for water works are stated in the Act 461/2000 and for small-scale households in the Act 401/2001 of the Finnish Ministry of Social Affairs and Health (Sosiaali- ja terveystieteiden ministeriö 2001). Both are based on the EU-directive, which again is based on the WHO's recommendations (European Parliament and Council Directive 1998). The water supply in general is handled by the Water Supply Act (119/2001).

The controlling authority concerning groundwater protection in Hanko is the environment protecting authorities of Hanko Town and the Uusimaa Regional Environment Centre. The controlling authority concerning drinking water is the health officer of Hanko. The protection of groundwater is also, promoted by information on the state of the groundwater for Hanko inhabitants by the authorities of Hanko.

The groundwater areas are classified in Finland in three different categories: areas important for water supply (class I), areas suitable for such use (class II), and other groundwater areas (class III) (Britschgi and Gustafsson 1996). The mapping

of these areas is done by Regional Environment Centres and the high quality maps of the groundwater areas are the basis for protection.

Concerning groundwater protection, the most important are class I areas and especially groundwater works and the catchments around them. The studied Hanko aquifer is locally a very important groundwater area and belongs to class I. Also the groundwater areas that are potential for new groundwater works are significant for protection. In the Hanko aquifer the most important area for protection is the area of the Hopearanta water works. Searching for new water resources to supply Hanko could be done by drilling new producing wells in a deeper location and further from the coast. The shallow groundwater aquifer is thickest in NW-SE trend from the Lindnäsudden area (Figure 6). Toward the mainland, the thickness of the sand and gravel deposit is up to 58 m and the groundwater depth range between less than 3 and 12 m below the surface. Sufficient information of sedimentation pattern of the sand and gravel formations of the groundwater aquifer would support the best location for the new wells and optimize the groundwater supply in the long term.

The use of artificially recharged groundwater is increasing in many parts of Finland. However, the artificial recharge could be very difficult for the Hanko area, due to the lack of close water resources. This would cause a high investment for the Hanko Town.

Crystalline bedrock forms the basement of the younger deposits and is distributed throughout the Hanko peninsula. The depth of bedrock varies from 30m below sea level to the surface level. Groundwater in the bedrock is accumulated along the fracture zones. The drilling operations to explore these groundwater resources are certainly more expensive than the shallow groundwater. Drilled bedrock groundwater wells in coastal areas also face the potential risk of the saltwater intrusion or relict salt water from the former Littorina Sea.

A plan concerning groundwater protection in Hanko was prepared in 1997 and was updated in 2005 (Harju 1997; Maa ja Vesi 2005). The plan was extensive and consists of a description of groundwater conditions, groundwater resources, potential risk functions and proposal for actions, groundwater quality, groundwater monitoring, and recommendations in restrictions of land use, provisions for crisis and actions in emergency. It is aimed as a base plan and regular procedure for a groundwater protection practice.

To protect shallow groundwater aquifers along the coastline, groundwater monitoring is needed and this should be done for both of groundwater quantity and quality. The monitoring of groundwater levels in shoreline areas, especially in the area nearby the main water work also requires information on the sea level. As the shallow groundwater in Hanko area is vulnerable to the intrusion of seawater, a routine monitoring will minimize the risk, e.g. chloride is an indicator of the intrusion of seawater. Monitoring will keep the groundwater quality situation in general updated. The remediation of groundwater is enormous and expensive work, so it is better to know the situation before the contamination reaches the water works' wells. Moreover, the monitoring will provide basic information of the groundwater condition and the groundwater budget balance between use, discharge and recharge and also on pumping control. In Hanko the monitoring of groundwater levels in observation wells around the water works is carried out, but the water quality in these wells is not monitored.

Climate change needs to be included in the water management plan and infrastructures (e.g. water supply net work, raw water treatment and water work), strategic planning and significant capital investments, management of supplies during droughts or flooding. Because climate change effects are still uncertain and difficult to evaluate, conceptual models of water cycle are crucial, therefore, strategic planning and management should be flexible to deal with the latest information and scheme for a scenario-based approach on the short, medium and long term. However, it is possible to manage with a certain amount of changes in water quantity or quality within existing operating practices such as some factors can be assessed monitoring, e.g. concentration of chloride in the groundwater and the groundwater level. In terms of infrastructure, routine inspection of the water distribution pipe network or use of long life span material for the pipe network, ensure sustainability.

Tools for good management of risks are already available in modern and forward-looking legislation, and by groundwater protection plans. The resources for controlling them are, however, limited. Economic limits confine, also the renewal of the sewer system and the freshwater system network. Most of the risks to groundwater discussed in section 6.4 above are known in Finland, except the effects of climate change and salt intrusion caused by the over pumping of groundwater. On the other hand, under the Environment Protection Act it is forbidden to do or to have much kind of new functions in important groundwater areas. For example it is forbidden to establish a new landfill in an important groundwater area. There are, however, remnants of old ones, such as the old Stormossen landfill in the Hanko aquifer area. Such existing functions, established before the new Act, are uncontrollable and therefore difficult to manage.

6.6 ADAPTATION OF GROUNDWATER PROTECTION STRATEGY IN HANKO AND OTHER COASTAL AQUIFERS IN FINLAND

Coastal aquifers

The risks to groundwater quantity or quality are much the same all over Finland. The vicinity of the Baltic Sea coast poses, however, a special threat to groundwater. The number of coastal aquifers is up to 600 from total of 12 982 aquifers in the whole country (Britschgi and Gustafsson 1996), so this problem exists for a large amount of aquifers. The changes in seawater level influence the groundwater level, and seawater may intrude into the freshwater aquifer. The sea salt may increase the salt content in precipitation and by infiltration the salt may reach the groundwater and affect on the quality. Also, the salt water increases the corrosion of materials in buildings or in freshwater pipelines or in sewer water pipelines that are in contact with salt water.

The detailed plan for groundwater protection is the most significant tool in the risk assessment and risk management. The plan should be prepared accurately and all the special factors based of the vicinity of sea should be considered. To this effect, a conceptual model for protection of shallow groundwater aquifer lying in coast area of Baltic Sea is presented in Figure 12.

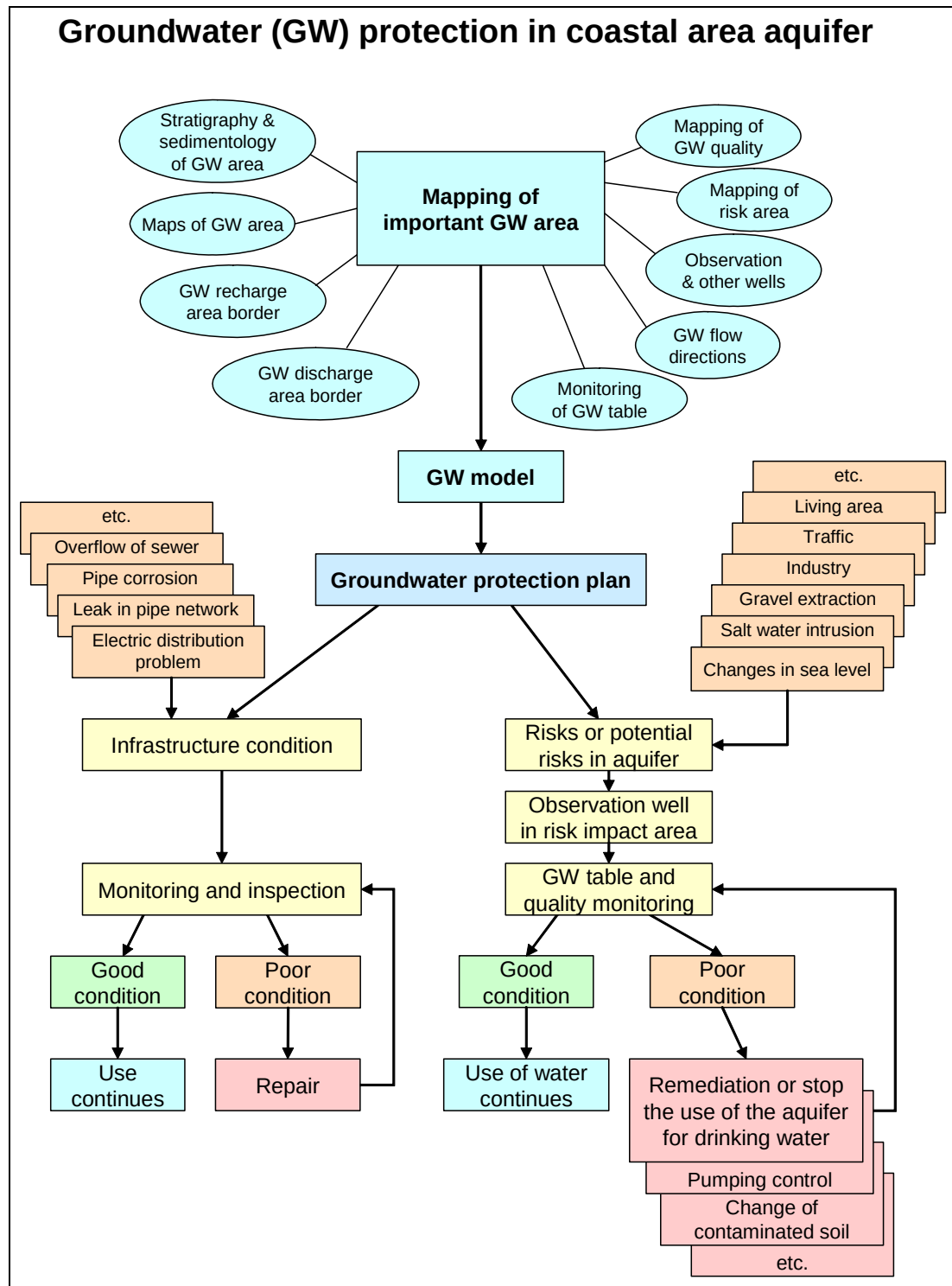


Figure VI—12 Groundwater (GW) protection strategy in coast area aquifer.

Adaptation strategies

Lack of water, especially from high quality groundwater would mean a crisis for all relevant users, such as residents and industrial sectors. Increasing cooperation among administration, industrial and other relevant sectors on the strategies of

groundwater protection is needed and can be done by increasing awareness of an importance to protect groundwater resources, hinder pollution and remediate possibly contaminated aquifers.

Detailed studies of stratigraphy in aquifers and groundwater flow models, groundwater recharge and discharge, in correspondence to either the present climate situation or the different scenarios due to climate change, have to be done. Also, the detailed mapping of all risks or potential risks may be constructed. Groundwater level and groundwater quality monitoring in range of the contaminant is significant. Monitoring includes also biological and microbiological monitoring, especially during long hot dry summers. New technologies in online measurements have progressed substantially in recent years, so automatic monitoring is a good option.

Concrete short and long term strategies on potential economic and environmental effects have to be taken into account. Long term investment and management plans for the infrastructure of the water supply and management, such as use of more durable material and long life span for the water supply network, can ensure capacities for the unforeseen effects of the climate change in the near future.

On a larger scale, groundwater issue is not solely local or national in the cross-border aquifer areas, such as in eastern Finland, where the groundwater aquifer from the First Salpausselkä formation extends to Russia. In these cases, cooperation on the groundwater management between countries is needed.

6.7 CONCLUSION

The risks and threats concerning shallow groundwater aquifers or water supply infrastructure are much the same all over Finland. The risks and threats are groundwater contamination caused by different factors, over pumping; diminish in recharge due to the increase of asphalt covers on the top of the aquifer, changes in recharge depending on changes in air temperature or in precipitation. The aquifers on the coastal areas have in addition to those also risks and threats caused by the vicinity of the sea: changes in groundwater level due to sea water level changes, intrusion of salt water into the aquifer, etc. These risks are being assessed just recently and the preparation for these risks is yet new and requires further development.

There are up to 600 aquifers from a total of 12,982 (Britschgi and Gustafsson 1996) in Finland located in the coast area. Changes in sea water level affect mainly the aquifers in South Finland and thus also the water supply in these areas. On the West coast area of Finland, the land uplift will compensate almost part of the affect of sea level changes. According to the Fourth Assessment Report (FAR) of the Intergovernmental Panel on Climate Change (IPCC 2007) and the sea level rise model of the SEAREG project, the sea level rise in Hanko coastal area would possibly reach 2.64 m by the end of 2100 based on the high case scenario. This could hinder or prevent the water supply and management in Hanko and in many other coast area aquifers. All the changes concerning water supply infrastructure are expensive and take time to realize.

In order to assess the new risks and threats, it is essential and leads to the establishment of a new risk management scheme. This study discussed the risk assessment and risk management in case study of Hanko and the aim was to pay attention to the factors that should be taken into account when a groundwater protection plan is prepared. The operation model presented by the study could be adapted to other similar coastal aquifers.

BIBLIOGRAPHY

Note: All websites referred to below last accessed in September 2007.

ABELE-WIGERT, ISABELLE AND MYRIAM DUNN (2006). *International CIIP Handbook 2006 VOL 1. An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*. Series editors Andreas Wenger and Victor Mauer. ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich.

ABELE-WIGERT, ISABELLE (2006). Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspective. In: MYRIAM DUNN AND VICTOR MAUER, EDS. (2006). *International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects*. Series editors Andreas Wenger and Victor Mauer. ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich, pp. 139-167.

AET (2007). *AET Umweltplanung GmbH: Rüstungsaltslasten an der Ostseeküste. Aktuelle Informationen über das Phosphorproblem auf Usedom*. Available at: www.aet-umweltplanung.de/brandopfer-usedom.htm

AISCAT (2006). *AISCAT position paper on: European Commission's Green Paper on a European Programme for Critical Infrastructure Protection*. Rome January 2006. Available at: www.aiscat.it/pubblicazioni/ue_news/ec_green_paper_on_critical_infrastructure_protection_aiscat_p.pdf

ALBERT, C. ET AL. (2003). *Introduction to the OCTAVE Approach*. CERT/Carnegie Mellon University.

ALEXA (2007). *10 most popular sites on the internet*. Available at: http://www.alexa.com/site/ds/top_500

AMERICAN CHAMBER (2006). *Position Paper on the Green Paper on Critical Infrastructure Protection*. American Chamber of Commerce to the European Union. Available at: www.eucommittee.be/Pops/2006/greenpaperoncriticalinfrastructure16012006.pdf

ANDERSON, K. V. (2002). Public Sector Process Rebuilding Using Information Systems. In: TRAUNMÜLLER, R. and LENK, K., ed, 2002. *Lecture Notes In Computer Science*, Vol. 2456, *Proceedings of the First International Conference on Electronic Government*, pp. 37-44.

ANDERSON, R. AND T. MOORE (2006) *The Economics of Information Security. Science*, Vol. 314, pp. 610-613.

- ANDERSSON, JAN JOEL AND ANDREAS MALM (2006). Public-Private Partnerships and the Challenge of Critical Infrastructure Protection. In: MYRIAM DUNN AND VICTOR MAUER, EDS. (2006). *International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects*. Series editors Andreas Wenger and Victor Mauer. ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich, pp. 139-167.
- ARECI (2007). *Availability and Robustness of Electronic Communications Infrastructures. Final report*. Available at: www.bell-labs.com/ARECI
- ASSAF, D. (2007). *Conceptualizing the use of public-private partnerships as a governing mechanism in critical information infrastructure protection. Conference on Non-State Actors as Standard Setters: The Erosion of the Public-Private Divide*, Basel Institute on Governance, Basel, Switzerland. February 2007.
- ASTRA (2007). *Developing Policies and Adaptation Strategies to Climate Change in the Baltic Sea Region*. Available at: <http://www.astra-project.org/cms/>
- AUDESTAD, J. A. (2005). Four Reasons Why 100 % Security Cannot be Achieved. *Teletronikk*. Issue 1, pp. 38-47.
- AUERSWALD, P. ET AL. (2005). The Challenge of Protecting Critical Infrastructure. *Issues In Science and Technology* Online, Issue 22. Also In: AUERSWALD, P. ET AL., ED. 2006. *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. New York: Cambridge University Press.
- AUSTRALIAN OFFICE OF TRANSPORT AND SECURITY (2004). *Offshore Oil and Gas Risk Content Statement*. Canberra. 2005.
- BA STRALSUND/BSH (2007). *Voraussichtlicher Untersuchungsrahmen für die Umweltverträglichkeitsstudie gemäß §6 UVPG im Rahmen des Genehmigungsverfahrens nach § 133 Abs.1 Nr.2 BBergG und § 43 EnWG für Errichtung und Betrieb der Transitgasrohrleitung „Nord Stream“*. Stralsund / Hamburg.
- BACKMAN, B. (2004). *Groundwater quality, acidification, and recovery trends between 1969 and 2002 in South Finland*. Geological Survey of Finland, Espoo. Bulletin 401.
- BAILAS, A. (2006). *Information Security Systems vs. Critical Information Infrastructure Protection — Similarities and Differences*. Proceedings of the International Conference on Dependability of Computer Systems (DEPCOS-RELCOMEX'06) May 2006.
- BALTIC MASTER (2007). *Maritime safety across borders. Reports and results*. Available at: http://www.balticmaster.org/file_archive.aspx?page_id=166
- BERLINER SALON E.V. (2007). *Rettet die Ostsee*. Berliner Salon e.V. Berlin 2006.
- BIJKER, R. (2000). Proven North Sea Solution Achieving Subsea Pipeline Burial And Stability With Spoilers. *Pipeline and gas journal*. April issue 2000.

- BISHOP, D. (2001). Coming to America: TETRA-One way or the other. *Mobile Radio Technology Magazine*, 1 January 2001. Available at: http://mrtmag.com/mag/radio_coming_america_tetraone/
- BOIN, ARJEN AND ALLAN MCCONNELL (2007). Preparing for critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need of Resilience. *Contingencies and Crisis Management*, Volume 15 Number 1, March 2007, pp. 50-59.
- BREILIN, O., M. PAALIJÄRVI AND T. VALJUS (2004). *Pohjavesialueen geologisen rakenteen selvitys I Salpausselällä Hanko–Lappohja alueella*. Geologian tutkimuskeskus, Espoo. Raportti 11 May 2004.
- BRITSCHGI, R. AND J. GUSTAFSSON, EDS. (1996). *Suomen luokitellut pohjavesialueet* (The classified groundwater areas in Finland, in Finnish with Swedish and English summaries). Finnish Environment Institute 55.
- BROWN, GERALD, MATTHEW CARLYLE, JAVIER SALMERÓN, KEVIN WOOD (2006). Defending Critical Infrastructure. *Interfaces* Vol. 36, No. 6, November–December 2006, pp. 530–544.
- BSH (BUNDESAMT FÜR SEESCHIFFFAHRT UND HYDROGRAPHIE) (2006). *Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline*. Hamburg.
- BSR INNONET (2007). Project information available at: <http://www.proinno.net/>
- BURNETT, D. (2006). *Underwater Infrastructure Protection, Risk Mitigation, and Pro-active Prosecution*. New York.
- BUYYA, R. ET AL. (2003). The Virtual Laboratory: A Toolset to Enable Distributed Molecular Modelling for Drug Design on the World-Wide Grid. *Concurrency and Computation: Practice and Experience*, Vol. 15, Issue 1, pp. 1-25.
- CALIN, D. ET AL. (2006). MAGNET: An Approach for Secure Personal Networking in Beyond 3G Wireless Networks. *Bell Labs Technical Journal*, Vol. 11, No. 1, pp. 79-98.
- CENTRAL INFORMATION SYSTEMS SECURITY DIVISION. (2005). *EBIOS – Expression of Needs and Identification of Security Objectives*. Available at: <http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html>
- CERT (2003). OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Available at: <http://www.cert.org/octave/>
- CLEANER SEAS (2007). Maritime safety and environmental concern are in high priority in VTT's research folde. Available at: http://www.vtt.fi/inf/julkaisut/muut/2007/Cleaner_Seas.pdf
- CMEX (2007). *Mars Exploration Concept Maps. A detailing various aspects of Mars exploration*. Center for Mars Exploration. Available at: <http://cmex.ihmc.us/cmex/table.html>

- COMMISSION (2000). Commission of the European Communities.
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*. Brussels, xxx COM(2000) 890 final.
- COMMISSION (2004). Commission of the European Communities.
Communication from the Commission to the Council and the European Parliament. *Critical Infrastructure Protection in the Fight Against Terrorism*. Brussels, 20.10.2004. COM(2004) 702 final.
- COMMISSION (2005a). *Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system* {SEC(2005) 1514} Available at:
<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0589:EN:NOT>
- COMMISSION (2005b). Commission of the European Communities 2005. *Green Paper on a European Programme for Critical Infrastructure Protection*. Brussels, 17.11.2005. COM(2005) 576 final. Available at:
www.uitp.com/mos/positionspapers/28-en.pdf
- COMMISSION (2005c). *Gas Priority Project in the European Union and in Neighbouring Countries*. Commission of the European Communities. DG Energy and Transport. Available at:
http://ec.europa.eu/ten/energy/studies/index_en.htm.
- COMMISSION (2006a). Commission of the European Communities 2006. *Proposal for a Directive of the Council on Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection*. Brussels, 12.12.2006. COM(2006) 787 final.
- COMMISSION (2006b). Communication on Protecting Europe's Critical Energy and Transport Infrastructure. DG Energy and Transport, European Commission. *Power Point presentation* 15 December 2006. Available at:
ec.europa.eu/dgs/energy_transport/security/infrastructure/doc/2006_12_15_presentation_en.pdf
- COMMISSION (2006c). Communication from the Commission of 31 May 2006: *A Strategy for a Secure Information Society – “Dialogue, Partnership and Empowerment”* [COM(2006) 251 final - not published in the Official Journal]. Available at: <http://europa.eu/scadplus/leg/en/lvb/l24153a.htm>
- COMMISSION (2007a). *Communication on Protecting Europe's Critical Energy and Transport Infrastructure*. DG Energy and Transport. Available at:
ec.europa.eu/dgs/energy_transport/security/infrastructure/doc/2006_12_15_presentation_en.pdf
- COMMISSION (2007b). *Commission takes first step towards improving critical infrastructure protection*. DG Energy and Transport European Commission.

- Press Release. Brussels, 2 February 2007. Available at:
<http://www.europa.eu/rapid/pressReleasesAction.do?>
- COPENHAGEN AGREEMENT (1971): *Copenhagen Agreement – Nordic Cooperation for the marine environment*. Available at:
<http://www.copenhagenagreement.org/>
- CORAS (2006). CORAS project (IST-2000-25031), information. Available at:
<http://coras.sourceforge.net/>
- COUNCIL (1999). Article 44 of Schengen acquis as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999. Council of the European Union. *Official Journal of the European Communities*.
- COUNCIL (2004). *EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks* (revised/widened CBRN Programme). Council of the European Union. Brussels, 1 December 2004, 15480/04.
- CRAMM (2006). *CRAMM toolkit*. Available at: <http://www.cramm.com/>
- CRITICAL INFRASTRUCTURE PROTECTION IN GERMANY (2005). Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) BSI/KRITIS.
- DAVENPORT, T. H. AND SHORT, J. E. (1998). The New Industrial Engineering: Information Technology and Business Process Redesign. *IEEE Engineering Management Review*, pp. 46-60.
- DE BRUIJNE, M. AND M. VAN EETEN (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management* Vol. 15, No. 1, pp. 18-29.
- DENMARK'S REPOSE (2006). *Denmark's response to the Green Paper on a European Programme for Critical Infrastructure Protection*. The European Commission, DG JLS Date 30 January 2006. Available at:
<http://www.beredskabsstyrelsen.dk/soeg/soeg.html?query=denmark%27s+response+&submit.x=0&submit.y=0&submit=submit>
- DER DERIAN, J. (2001). 9-11: *NETWAR and MIME-NET*. The Information Technology, War and Peace Project. Available at:
<http://www.watsoninstitute.org/infopeace/911/index.cfm?id=5#>
- DER TAGESSPIEGEL (2007). Explosion zerfetzt Gaspipeline. *Der Tagesspiegel*. Berlin. 7. May 2007.
- DNV (2006). *Det Norske Veritas, Pipeline Damage Assessment from Hurricane Ivan in the Gulf of Mexico*. Houston.
- DOCTRINE OF THE INFORMATION SECURITY OF THE RUSSIAN FEDERATION (2000). President of the Russian Federation Vladimir Putin 9 September 2000, No. Pr-1895.
- DRITTER GEFAHRENBERICHT DER SCHUTZKOMMISSION (2006). *Dritter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern Bericht über mögliche Gefahren für die Bevölkerung bei Großkatastrophen*

- und im Verteidigungsfall*. März 2006. Schriftenreihe der Schutzkommission beim Bundesminister des Innern. Herausgegeben vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe im Auftrag des Bundesministeriums des Innern. Neue Folge Band 59.
- DUKE CORPORATE EDUCATION (2005). *Translating Strategy into Action*. Kaplan Business, Dearborn Trade Publishing.
- DUNN, MYRIAM (2006). Understanding Critical Information Infrastructure: An Elusive Quest. In: MYRIAM DUNN AND VICTOR MAUER, EDS. (2006). *International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects*. Series editors Andreas Wenger and Victor Mauer. ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich, pp. 27-40.
- DUNN, MYRIAM AND ISABELLE WIGERT (2004). *International CIIP Handbook 2004. An Inventory and Analysis of Protection Policies in Fourteen Countries*. Zurich: Swiss Federal Institute of Technology.
- DUNN, MYRIAM AND VICTOR MAUER, EDS. (2006). *International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects*. Series editors Andreas Wenger and Victor Mauer. ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich.
- EAPC (2003). *EAPC Critical Infrastructure Protection – Concept Paper*. 10 November 2003.
- ECEIA (1991). *Espoo Convention on Environmental Impact Assessment in a Transboundary Context*. Espoo 1991. Available at: <http://www.unece.org/env/eia/eia.htm>
- ECKSTRÖM, A. H. (2004). *Teleavbrottet i Uppsala 2002 – Infrastrukturell sårbarhet*. Försvarshögskolan (Swedish National Defence College). Stockholm.
- EGAN, MATHEW JUDE (2007). Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Contingencies and Crisis Management*, Volume 15 Number 1, March 2007, pp. 4-17.
- EICTA COMMENTS (2006). *EICTA comments to the Commission Green Paper on a European Programme for Critical Infrastructure protection*. Available at: http://eicta.ntc.be/index.php?id=33&id_article=71
- EIIP VIRTUAL FORUM (2006). *GAO Reports on DHS Implementation of Critical Infrastructure Information Act*. Available at: <http://www.emforum.org/news/06051701.htm>
- EMARKETER (2007). *European E-Commerce to Reach 323 Billion Euros in 2011*. Available at: <http://www.marketingcharts.com/direct/european-e-commerce-to-reach-323-billion-euros-in-2011-1239/>
- ENERGIATEOLLISUUS (2006). *Kommentteja komission julkaisemaan vihreään kirjaan kriittisen. infrastruktuurin suojeleuhjelman tarpeellisuudesta*,

- sisällöstä ja sitouvuudesta. Lausunto kriittisen infrastruktuurin suojeleuhjelmasta. Energiateollisuus. Kaukolämpö. Energiateollisuus ry.*
- ENISA (2007). *Inventory of CERT activities in Europe*. Available at: http://www.enisa.europa.eu/cert_inventory/index_inventory.htm .
- ERHENFELD, R. (2002). *Funding Terrorism: Sources and Methods*. Presented at workshop on Confronting Terrorism. Los Alamos Laboratory.
- ESPO (2006). *European Sea Ports Organisation. Green Paper on Critical Infrastructure, ESPO's initial views*. Available at:
- ESSENWANGER, O. M., 2001. *Classification of Climates*. World Survey of Climatology 1C, General Climatology. Amsterdam: Elsevier.
- ET ROBUST OG SIKKERT SAMFUND REGERINGENS POLITIK FOR BEREDSKABET I DANMARK (2005). Regeringen. Juni 2005. Publisher: Forsvarsministeriet [Ministry of Defence].
- ETSI EN (2007a). Voice plus Data (V+D); Part 7: Security, *ETSI EN 300 392-7 V3.0.2*.
- ETSI EN (2007b). Voice plus Data (V+D); Part 2: Air Interface (AI), *ETSI EN 300 392-2 V3.2.0*.
- ETSI TR (2007). Terrestrial Trunked Radio (TETRA). User Requirement Specification TETRA Release 2. TR 102 021 series. Available at: <http://www.etsi.org/WebSite/technologies/Emergency.aspx>
- EUROBALTIC GUIDELINES (2007). *Does Your Community Have an Injury Prevention Programme? Eurobaltic Guidelines for Safety Promotion in the Baltic Sea Region*. Author: Christer Pursiainen. Nordregio and Swedish Rescue Services Agency. November 2007.
- EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE., (1998). *Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption*. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0083:EN:HTML>
- EUTELIS (1998). *Recommended Practices for Collocation and Other Facilities Sharing for Telecommunications Infrastructure*. Consortium for DG XIII of the EC.
- EXECUTIVE ORDER (1996). *Executive Order EO 13010. Critical Infrastructure Protection*. The White House. July 15, 1996.
- FAWAZ, G. ET AL. (2004). Service level agreement and provisioning in optical networks. *IEEE Communications Magazine*, Vol. 42, No. 1, January 2004.
- FECC (2006). *FECC European Association of Chemical Distributors. FECC's comments to the Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP)*.
- FILDES, J. (2006). Keep Connected. *BBC News online article*. Available at: http://news.bbc.co.uk/1/hi/newsid_5140000/5140358.stmbject
-

- FIMR (2007). FINNISH INSTITUTE OF MARINE RESEARCH, *Wave and sea level*. Available at: <http://www.fimr.fi/en/palvelut/aallokko-ja-vedenkorkeus.html>
- FINEXTRA (2007). *M-commerce market to grow to \$40bn by 2009*. Available at: <http://www.finextra.com/fullstory.asp?id=12605>
- FINGRID (2007a). *State of power system*. Available at: http://www.fingrid.fi/portal/in_english.
- FINGRID (2007b). Available at: http://www.fingrid.fi/portal/in_english/electricity_market/state_of_power_system/
- FINNISH CUSTOMS (2005). *Annual Report 2005*. Available at: http://www.tulli.fi/en/02_Publications/03_Annual_reports/Annual_Report_2005.pdf
- FINNISH CUSTOMS (2006). *Annual Report 2006*. Available at: http://www.tulli.fi/en/02_Publications/03_Annual_reports/Annual_Report_06.pdf
- FINNISH ENERGY INDUSTRIES (2007). Available at: <http://www.energia.fi/EN>
- FINNISH MINISTRY OF THE ENVIRONMENT (2007). *Answer to the notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline*. Helsinki, 16 February 2007.
- FITZDUFF, MARI (1989). *A Typology of Community Relations work and Contextual necessities*. Belfast: Policy and Planning Unit, Northern Ireland Office.
- FITZDUFF, MARI (2004). Meta-Conflict Resolution. In: GUY BURGESS AND HEIDI BURGESS, EDS., *Beyond Intractability*. Conflict Research Consortium, University of Colorado, Boulder. Posted: September 2004. Available at: <http://www.beyondintractability.org/essay/meta-conflict-resolution/>
- FMI (2007). *Climate in Finland*. Finnish Meteorological Institute. Available at: <http://www.fmi.fi/weather/climate.html>
- FOI (2007). *Sweden and Baltic Sea Security*. Swedish Defence Research Agency: Nord Stream. Stockholm.
- FORSTEN J. AND M. LEHTONEN (2001). *Sähkön toimitusvarmuuden parantaminen*. Kauppa- ja teollisuusministeriö.
- FREEZE, R.A. AND J.A. CHERRY (1979). *Groundwater*. Englewood Cliffs: Prentice-Hall.
- FRITZON, ÅSA, KRISTIN LJUNGKVIST, ARJEN BOIN AND MARK RHINARD (2007). Protecting Europe's Critical Infrastructures: Problems and prospects. *Contingencies and Crisis Management*, Volume 15 Number 1, March 2007, pp. 30-41.

- FUNDAMENTALS OF COUNTER-TERRORISM IN ESTONIA (2006).
Approved by Resolution no. 15 of Minutes no. 38 of the Government of the Republic session of 17.08.2006.
- FYFE, G. J. (1991). *The morphology and sedimentology of the Salpausselkä I Moraine in southwest Finland*. Cambridge University : Fitzwilliam College.
- GALBRAITH J. (2007). *Jay Galbraith's Star Model™*. Available at:
http://www.jaygalbraith.com/star_model.asp
- GARLIK (2007). *The Garlik UK Cybercrime Report*, August 2007. Available at:
<https://www.garlik.com/press/Garlik%20Cybercrime%20Report.pdf>
- GEOLOGICAL SURVEY OF FINLAND (2006). *The spatial effects and management of natural and technological hazards in general and in relation to climate change*. European Spatial Observation Network (ESPON) project 1.3.1. Available at: <http://www.gtk.fi/projects/espon/>
- GEORGE MASON UNIVERSITY (2007). *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*. CIP Program Discussion Paper series. Virginia: George Mason University.
- GHEORGHE, AV., M. MASERA. M. WEIJNEN AND L. DE VRIES (2006), *Critical Infrastructures at Risk. Securing the European Electric Power System*, Netherlands: Springer.
- GILLIS, T. (2007). *Internet Security Trends for 2007: A Report on Spam Viruses and Spyware*. IronPort Systems.
- GORDON, S. (2003). *Virus and Vulnerability Classification Schemes: Standards and Integration*. Symantec white paper.
- GOTH, G. (2007). Fast-Moving Zombies: Botnets Stay a Step Ahead of the Fixes. *IEEE Internet Computing*. Vol. 11, Issue 2, pp. 7-9.
- GRAHAM, R. AND D. MAYNOR (2006). *SCADA Security and Terrorism: We're Not Crying Wolf*. Presentation at Blackhat Federal.
- GRANGER, S. (2006). *Social Engineering Reloaded*. Available at:
<http://www.securityfocus.com/infocus/1860>
- GREATER LONDON AUTHORITY. (2006). *Report of the 7 July Review Committee*. June 2006.
- GREENEMEIER, L. (2007). 'Electronic Jihad' App Offers Cyberterrorism for the Masses. *Information Week*. Available at:
<http://www.informationweek.com/story/showArticle.jhtml?articleID=200001943>.
- GSM WORLD (2007). *GSM World statistics*. Available at:
<http://www.gsmworld.com/gsmastats.shtml>
- GUIDE FOR ALL-HAZARDS EMERGENCY OPERATIONS PLANNING (1996). State and Local Guide (SLG) 101. Federal Emergency Management Agency (FEMA). September 1996.

- HAGELSTAM, AXEL (2005). *CIP – Kriittisen infrastruktuurin turvaaminen. Käsiteanalyysi ja kansainvälinen vertailu*. Huoltovarmuuskeskus. Julkaisuja 1/2005. Huoltovarmuuskeskus. Helsinki.
- HÄNNINEN, SAARA AND JORMA RYTKÖNEN (2004). *Oil transportation and terminal development in the Gulf of Finland*. VTT Publications: 547. VTT Industrial Systems. Espoo. Available at: www.vtt.fi/inf/pdf/publications/2004/P547.pdf
- HARJU, P. (1997). *Hangon pohjavesialueiden suojelusuunnitelma* (Protection plans for groundwater areas in Hanko, in Finnish). Uudenmaan ympäristökeskus. Monisteita 22.
- HATVA, T., J. HYYPPÄ, J. IKÄHEIMO, J., H. PENTTINEN AND M. SANDBORG (1993). *Soranoton vaikutus pohjaveteen. Raportti VI: Pohjavesi ja soranotto* (The impact of gravel extraction on groundwater - Report VI: Groundwater and gravel extraction, in Finnish with English summary). Ympäristöministeriö. Kaavoitus- ja rakennusosasto. Tutkimusraportti 1.
- HELCOM (1994). *Helsinki Commission: Report to the 15th Meeting of Helsinki Commission 8 - 11 March 1994 from the Ad Hoc Working Group on Dumped Chemical Munition* (HELCOM CHEMU), Helsinki.
- HELCOM (2004a). *30 years of protecting the Baltic Sea - HELCOM 1974-2004*. Available at: http://www.helcom.fi/stc/files/Publications/OtherPublications/30_years_jubilee.pdf
- HELCOM (2004b). *Recommendation 25/7: Safety of Winter Navigation in the Baltic sea Area*. Available at: http://www.helcom.fi/Recommendations/en_GB/rec25_7/
- HELCOM (2005). *HELCOM Response 6/2005*. HELSINKI COMMISSION Response Group Sixth Meeting Klaipeda, Lithuania, 30 November - 2 December 2005.
- HELCOM (2006a). *HELCOM Activities 2006. Overview*. Baltic Sea Environment Proceedings No. 112. Available at: <http://www.helcom.fi/stc/files/Publications/Proceedings/bsep112.pdf>
- HELCOM (2006b). *Maritime Transport in the Baltic Sea, Draft*. HELCOM. Thematic Assessment in 2006, 3. Available at: <http://sea.helcom.fi/dps/docs/documents/Ad%20hoc%20Task%20Force%20for%20HELCOM%20BSAP/HELCOM%20BSAP%20TASK%20FORCE%201%202006/3-3.pdf>
- HELCOM (2007). *Climate Change in the Baltic Sea Area – HELCOM Thematic Assessment in 2007*. Baltic Sea Environment Proceedings No. 111. Helsinki. Available at: <http://www.helcom.fi/stc/files/Publications/Proceedings/bsep111.pdf>
- HELLENBERG, TIMO AND SIGRID HEDIN (2006). *Cross-border risks in the Baltic Sea Region. Lessons to be learned*. Eurobaltic Publications 4. Multiprint Oy. Helsinki.

- HELLENBERG, TIMO (2006). Baltic Sea Energy Roulette: Is a Survival Kit on Civil Protection needed? Expert Article 73, *Baltic Rim Economies Bimonthly Review*. 6/2006. Pan-European Institute, Turku School of Economics.
- HERNAN, S. ET AL. (2006). Uncover Security Design Flaws Using The STRIDE Approach. *MSDN Magazine*.
- HS (2007a). Venäjän muutos tuntuu Suomenlahdella rajuna. *Helsingin Sanomat*, B 3, 4.3.2007.
- HS (2007b). Suomenlahden öljyvirta voi tuplaantua. *Helsingin Sanomat*, B 4, 5.3.2007.
- HS (2007c). Itäinen Suomenlahti varautuu suuren öljyturman seurauksiin. *Helsingin Sanomat*, A 4, 6.3.2007.
- HS (2007d). Silja Serenade vältti törmäyksen nipin napin Tukholman-reitillä. *Helsingin Sanomat*, 10.3.2007.
- HS (2007e). Venäjä suunnittelee Suomenlahdelle aiempaa suurempia öljytankkereita. *Helsingin Sanomat*, B 5, 11.6.2007.
- HUPKA, J. (2007). Technical aspects of gas pipeline operation. In: *Proceedings of the International Conference on Environmental Threats to the Baltic Sea held in Warsaw Sheraton Hotel*, 28 May 2007. Available at: www.senat.gov.pl/k6/agenda/seminar/070528e/indexer.htm
- HURLEY, DANIEL C. (2000). *Critical Infrastructure Protection: Roles of the Government and Private Sectors and Opportunities for Those Who Carry Out these Roles*. U.S. Department of Commerce, National Telecommunications and Information Administration.
- HYPONNEN, M. (2006). Malware Goes Mobile. *Scientific American*, pp. 70-77.
- IAGS (2005). *Pipeline Sabotage is Terrorist's Weapon of Choice*. Institute for the Analysis of Global Security. Available at: www.iags.org/n0328051.htm
- IET NEWS BREFING (2007). Estonia Looks to Cyber Defence, After Attacks. *Communications Engineer*, pp. 3, August/September.
- IMO (1971). IMO legislation, *Copenhagen Agreement 1971*.
- IMO (1972). *Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs)*. Available at: http://www.imo.org/Conventions/mainframe.asp?topic_id=257&doc_id=649
- IMO (1973): *International Convention for the Prevention of Pollution from Ships, 1973*, as modified by the Protocol of 1978 relating thereto (MARPOL 73/78). Annexes I, II, V. Available at: http://www.imo.org/Conventions/contents.asp?doc_id=678&topic_id=258
- IMO (1995): *International Convention on Oil Pollution Preparedness, Response and Co-operation, 1990. (OPRC)* Available at: http://www.imo.org/Conventions/mainframe.asp?topic_id=258&doc_id=682
- IMO (2002): *Resolution MSC 138(76) Recommendation On Navigation Through The Entrances To The Baltic Sea*. Available at:

http://www.imo.org/includes/blastDataOnly.asp/data_id%3D15508/138%2876%29.pdf

IMO Resolution A. 620(15), *Navigation through the Entrances to the Baltic Sea*.

IMO Resolution A. 978(24). *Amendments to the existing mandatory ship reporting system "In the Great Belt Traffic Area"* Available at:

http://www.imo.org/about/mainframe.asp?topic_id=1018&doc_id=5466#resos

INTERMINISTERIAL MEETING CONCERNING CRITICAL

INFRASTRUCTURE (2007). News 4 April 2007. Available at:

<http://www.mswia.gov.pl/portal.php?serwis=en&dzial=1&id=244&search=422959>

INTERNATIONAL CEP HANDBOOK (2006). *Civil Emergency Planning in the NATO/EAPC Countries*. SEMA's Educational Series 2006:1.

IPCC (2007). *Climate Change 2007: The Physical Science Basis, Summary for Policymakers*. Fourth Assessment Report, a Report of Working Group I, Intergovernmental Panel on Climate Change (IPCC), 18 p. Available at: <http://www.ipcc.ch/SPM2feb07.pdf>

IRGC (2005). *Critical Infrastructures. Fact Sheet*. International Risk Governance Council.

IRRIIS (2006). *IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems*. Available at: <http://www.irriis.org/>

ISBMSC (2007). *International Seminar on Baltic Maritime Safety Cooperation*. St. Petersburg, Russia, 5. - 6. June 2007. Available at <http://www.gofmec.fi/>

ITU-T (1991). Security architecture for Open Systems Interconnection for CCITT applications. ITU-T Recommendation X.800.

ITU-T (2003). Security architecture for providing end-to-end communications. ITU-T Recommendation X.805.

ITU- T (2007). Information available at: <http://www.itu.int/ITU-T/ngn/index.phtml>

JENKINS, W. I. (1978). *Policy Analysis: A Political and Organizational Perspective*. New York, St. Martin's Press.

JØRGENSEN, K.S., K. BJÖRKLÖF, E. SCHULTZ, J. SORVARI, J. SALMINEN, T. HUOTARI, J. REINIKAINEN, P. HÄNNINEN, J. LEVEINEN, M. HEINO, M. AND P. LINTINEN (2006). *Demonstration of the Use of Monitored Natural Attenuation (MNA) as a Remediation Technology - DEMO-MNA*. Finnish Environment Institute. Available at: <http://www.ymparisto.fi/default.asp?contentid=238101&lan=EN>

JUDITH, E.Y. ET AL. (2007). eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope. In: *Second International Conference on Availability, Reliability and Security (ARES'07)*, Vienna, pp. 925-933, 10-13 April 2007.

JUVONEN, J. (2005). *Integration of Emergency Response Centers*. Presentation at the 2nd TETRA South Korean Conference. 22 June 2005. Available at:

- http://www.tetramou.com/uploadedFiles/Files/Presentations/SK05_Juvonen.ppt.
- KARI, H. (2007). *Protecting Critical Information Infrastructures*. Lecture notes, National Defence University, Helsinki, 32 p., 1 April 2007. Available at: http://www.huoltovarmuus.fi/documents/7/2007-05-09_TIVA-ES-Kari.pdf.
- KASKEALA, J. (2006). *Finnish Approach to Homeland Security – Interagency Cooperation*. Presentation for NATO's Euro-Atlantic Partnership Council, 16 November 2006. Available at: http://www.mil.fi/liite/chod_fi_presentation_for_nato_eapc_final.pdf.
- KASPEREK, T. (2007). Threat to people posed by the removal of chemical ammunition dumped in the Bornholm depth. In: *Proceedings of the International Conference on Environmental Threats to the Baltic Sea held in Warsaw Sheraton Hotel*, 28 May 2007. Available at: www.senat.gov.pl/k6/agenda/seminar/070528e/indexer.htm.
- KENNING, M. J. (2001). Security Management Standard — ISO 17799/BS 7799. *BT Technology Journal*. Vol. 19, No. 3, pp. 132-136.
- KETTERLING, H. (2004). *Introduction to Digital Professional Mobile Radio*. Artech House, Boston.
- KIELOSTO, S., M. KUKKONEN, C.-G. STÉN, AND B. BACKMAN (1996). *Hangon ja Perniön kartta-alueiden maaperä*. Suomen geologinen kartta 1:100 000, maaperäkarttojen selitykset, lehdet 2011 ja 2012. Geologian tutkimuskeskus, Espoo, 1996.
- KIELY, L., AND T. BENZEL (2006). Systemic Security Management. *IEEE Security & Privacy*. Vol. 4, Issue 6, pp. 74-77.
- KIMBER, D. ET AL. (2006). Modeling Planned Downtime. *Bell Labs Technical Journal*. Vol. 11, No. 3, pp. 7-19.
- KINNUNEN, T., ED. (2006). *Pohjavesien suojelun ja kiviaineshuollon yhteensovittaminen - Uudenmaan ja Itä-Uudenmaan loppuraportti* (Accommodation between groundwater protection and aggregate supply - final report from Uusimaa and Itä-Uusimaa, in Finnish with Swedish and English summaries). Uusimaa Regional Environment Centre 400. 264 p. Available at: <http://www.ymparisto.fi/default.asp?contentid=187015&lan=fi>
- KROPP, J. (2007). *Climate Change Scenarios and costs of Sea-Level Rise in the Baltic Sea Region*. A presentation for the ASTRA project meeting in Tampere, Finland. Potsdam Institute for Climate Impact Research (PIK). Available at: http://www.astra-project.org/cms/sites/download/Tampere_kropp.pdf
- LAANET, K. (2007). *Interagency Radio Network of Estonia*. Estonia Minister of Interior's presentation at VIRVE Day 2007. Helsinki, 1 March 2007.
- LAAR, MART (2007). *The Estonian Economic Miracle*, The Heritage Foundation, August 7, 2007 August 7. Available at: <http://www.heritage.org/Research/WorldwideFreedom/bg2060.cfm>

- LAHERMO, P., T. TARVAINEN, T. HATAKKA, B. BACKMAN, R. JUNTUNEN, N. KORTELAINE, T. LAKOMAA, M. NIKKARINEN, P. VESTERBACKA, U. VÄISÄNEN, AND P. SUOMELA (2002). *Tuhat kaivoa - Suomen kaivovesien fysikaalis-kemiallinen laatu vuonna 1999*. (Summary: One thousand wells-the physical-chemical quality of Finnish well waters in 1999.) Geologian Tutkimuskeskus, Geological Survey of Finland. Espoo. Report of Investigation 155.
- LANDSTEDT, JYRKI AND PETTER HOLMSTRÖM (2007). *Electric Power Systems Blackouts and the Rescue Services: the Case of Finland*. CIVPRO Working Paper 2007:1.
- LEHTINEN, M., P. NURMI, AND T. RÄMÖ, EDS. (2005). Precambrian geology of Finland : key to the evolution of the Fennoscandian shield. *Developments in Precambrian Geology*, 14. Amsterdam: Elsevier. xiv, 736 p. ISBN 0-444-51421-X.
- LESK, M. (2007). The New Front Line: Estonia under Cyberassault. *IEEE Security & Privacy Magazine*, Vol. 5, Issue 4, pp. 76-79.
- LIBBENGA, J. (2007). Phishers Haul in Money from Nordic Bank. *The Register*. Available at:
http://www.theregister.co.uk/2007/01/19/phishers_attack_nordea/
- LIOTINE, M. (2003). *Mission-Critical Network Planning*. Boston: Artech House.
- LIUHTO KARI (2007). *A future role of foreign firms in Russia's strategic industries*. Electronic Publications of Pan-European Institute 4/2007, Turku School of Economics. Available at:
http://www.tukkk.fi/pei/verkkojulkaisut/Liuhto_42007.pdf
- LIUKKONEN, SEPPO (2006). *Technical requirements for year-round Baltic Sea tanker traffic*. Presentation in a conference on Ice Tanker Operations, Hamburg, 28th September 2006. Available at:
<http://www.thedigitalship.com/powerpoints/SMM06/ice/seppo%20liukkonen,%20GL.pdf>
- LUKASIK, STEPHEN J., SEYMOR E. GOODMAN AND DAVID W. LONGHURST (2003), *Protecting Critical Infrastructure Against Cyber-Attack*, Adelphi Paper 359, New York: Oxford University Press.
- MAA JA VESI, (2005). *Hangon pohjavesialueiden suojelusuunnitelman päivitys*. Hanko City and Uusimaa Regional Environment Centre.
- MARIUSSEN, ÅGE, AALBU, HALLGEIR AND BRANDT, MATS (2000). *Regional Organisations in the North*. Stockholm, Nordregio WP 2000:8.
- MARTTILA, V., H. GRANHOLM, J. LAANIKARI, T. YRJÖLÄ, A. AALTO, P. HEIKINHEIMO, J. HONKATUKIA, H. JÄRVINEN, J. LISKI, R. MERIVIRTA, AND M. PAUNIO (2005). *Ilmastomuutoksen kansallinen sopeutumisstrategia (Finland's National Strategy for Adaptation to Climate Change, in Finnish with Swedish and English abstracts)*. Maa- ja metsätalousministeriö (MMM) julkaisu 1/2005. 276 p. Available at:
http://wwwb.mmm.fi/julkaisut/julkaisusarja/2005/MMMjulkaisu2005_1.pdf

- MAZURKIEWICZ, B. (2007). Technical conditions of construction and operation of the gas pipeline on the bottom of the Baltic Sea. *In: Proceedings of the International Conference on Environmental Threats to the Baltic Sea held in Warsaw Sheraton Hotel*, 28 May 2007. Available at: www.senat.gov.pl/k6/agenda/seminar/070528e/indexer.htm.
- MEETING WITH CRITICAL INFRASTRUCTURE OPERATORS (2007). NEWS. National Civil Defence. Information Service. Available at: <http://ock.gov.pl/portal/oce/46/197/>
- MEIER, H.E.M., B. BROMAN, AND E. KJELLSTRÖM (2004). Simulated sea level in past and future climates of the Baltic Sea. *Climate Research* 27, pp. 59-79.
- MEIER, H.E.M., B. BROMAN, H. KALLIO, AND E. KJELLSTRÖM (2006). Projections of future surface winds, sea levels, and wind waves in the late 21st century and their application for impact studies of flood prone areas in the Baltic Sea region. *In: SCHMIDT-THOME, P., ED.: Sea Level Changes Affecting the Spatial Development of the Baltic Sea Region*. Geological Survey of Finland, Special Paper 41, 23-43.
- MERENTUTKIMUSLAITOS (2006). Aranda. Uutiset: Suomenlahden happikatoalue poikkeuksellisen laaja, pohjan tila heikempi kuin kertaakaan 2000-luvulla. Available at <http://www.fimr.fi/fi/aranda/uutiset/238.html>
- MERITURVALLISUUSSEMINAARI (2007). *Meriturvallisuusseminaari*, Finlandiatalo, Helsinki, Finland, 24.4.2007. Available at <http://www.vtt.fi>
- MILETI, DENNIS (1999). *Disasters by Design. A Reassessment of Natural Hazards in the United States*. Joseph Henry Press, Washington DC.
- MINISTRY OF THE INTERIOR (2004). *ISDR Country Report Finland*, August 23, 2004. Paper written by Mr. Taito Vainio for the Conference on Disaster Reduction held in Kobe-Hyogo in Japan in 18-22 January 2005. Available at: <http://www.unisdr.org/eng/mdgs-drr/national-reports/Finland-report.pdf>
- MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND (2004). *Creating a Safer Information Society*. Available at: [http://www.mintc.fi/oliver/upl502-NISAB%20report%20\(midres\).pdf](http://www.mintc.fi/oliver/upl502-NISAB%20report%20(midres).pdf)
- MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND (2005). *Transport connections between the EU and Russia. Current Status and Outlook for the Future*. Publications 10/2005. Available at: http://www.mintc.fi/oliver/upl255-Julkaisu%2010_2005.pdf
- MOGUL, R. (2002). Danger Within –Protecting your Company from Internal Security. *Attacks Gartner, CSO Magazine, Analyst Report*, 21. Available at: <http://www.csoonline.com/analyst/report400.html>
- MOND (1999). *Chemical Weapons Dumped in the Baltic Sea*. Polish Ministry of National Defence, Department of International Security. Warsaw.
- MOTEFF, JOHN, D. (2003). *Critical Infrastructures: Background, Policy, and Implementation*. Report for Congress. Received through the CRS Web. Order Code RL30153. Congressional Research Service. The Library of Congress.

- MOTEFF, JOHN (2004). *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and managing Threats, Vulnerabilities and Consequences*. CRS report for Congress. Received through the CRS Web. Order Code RL32561. Congressional Research Service. The Library of Congress.
- MOTEFF, JOHN AND PARFOMAK, PAUL (2004). *Critical Infrastructure and Key Assets: Definition and Identification*. CRS Report for Congress. Received through the CRS Web. Order Code RL32631. Congressional Research Service. The Library of Congress.
- MOTEFF, JOHN, COPELAND, CLAUDIA, FISCHER, JOHN (2003). *Critical Infrastructures: What makes an Infrastructure Critical?* Report for Congress. Received through the CRS Web. Order Code RL31556. Congressional Research Service. The Library of Congress.
- MTV3-STT (2007). *Öljyonnettomuuden riski kasvaa voimakkaasti Suomenlahdella*. MTV Internet News. 18.5.2007. Available at: <http://www.mtv3.fi/uutiset/kotimaa.shtml/arkistot/kotimaa/2007/05/528657>
- MUSSINGTON, DAVID (2002). *Concepts for Enhancing Critical Infrastructure Protection. Relating Y2K to CIP Research and Development*. Prepared for the Office of Science and Technology Policy. RAND Science and Technology Policy Institute.
- NAEDELE, M. (2007). *Addressing IT Security for Critical Control Systems*. Presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS). Jan 2007.
- NÅR SIKKERHETEN ER VIKTIGST (2006). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Innstilling fra utvalg oppnevnt ved kongelig resolusjon 29. oktober 2004. Avgitt til Justis- og politidepartementet 5. april 2006. NOU Norges offentlige utredninger 2006: 6. Departementenes servicesenter Informasjonsforvaltning. Oslo.
- NATIONAL SÅRBARHEDSRAPPORT (2006). Beredskabsstyrelsen.
- NATIONAL SECURITY CONCEPT OF THE REPUBLIC OF ESTONIA (2004). Available at: <http://www.libertysecurity.org/article963.html>
- NATIONAL SECURITY CONCEPT OF THE REPUBLIC OF LATVIA (2002). Approved in Parliament on 24.01.2002. Ministry of Foreign Affairs of Latvia, unofficial translation. Available at: http://www.mfa.gov.lv/en/security/basic/4534/?print=on#_Toc10954546
- NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF LITHUANIA (2002/2005). Approved by the Parliament of the Republic of Lithuania 28 May 2002, Decision No. ix-907. (Version of the Decision no. 2005. Parliament of the Republic of Lithuania).
- NATIONAL SECURITY CONCEPT OF THE RUSSIAN FEDERATION (2000). Approved by Presidential Decree No. 1300 of 17 December 1997, given in the wording of Presidential Decree No. 24 of 10 January 2000.

- NATO (2006). *NATO's Role in Civil Emergency Planning*. September 2006.
- NEHRING, S. (2006). Erdgas trifft Giftgas. Die explosiven Risiken der Ostseepipeline. *Der Rabe Ralf*, Heft August/September 2006.
- NEHRING, S. AND B. ILSCHNER (2005). Ostsee-Pipeline – ein explosives Vorhaben. Die unkalkulierbaren Risiken des neuen deutsch-russischen Erdgas-Projekts. *Waterkant*. ISSN 1611-1583, Heft 4 / 2005.
- NIPP (2006). *National Infrastructure Protection Plan*. U.S. Department of Homeland Security.
- NON-PAPER ON THE STEP-BY-STEP APPROACH TO THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (2006). Denmark, The Netherlands, Sweden, United Kingdom, Poland. Copenhagen 14 February 2006.
- NORD STREAM (2006a). Project Information Document. Offshore pipeline through the Baltic Sea. November 2006.
- NORD STREAM (2006b). *Gaspipeline von der Grenze der deutschen AWZ bis zum Anlandungspunkt am Kraftwerksstandort Lubmin*. Institut für Angewandte Ökologie GmbH: Scoping-Unterlage für die Nord Stream.
- NORD STREAM (2007). *Gasunie and Gazprom Agree on Nord Stream Terms*. 06 November 2007. Available at :
[http://www.nordstream.com/news_detail.html?&no_cache=1&tx_ttnews\[tt_news\]=312&tx_ttnews](http://www.nordstream.com/news_detail.html?&no_cache=1&tx_ttnews[tt_news]=312&tx_ttnews)
- NORDEA FINLAND (2007). *Important security information*. Nordea Finland. Available at:
<http://www.nordea.fi/Personal+customers/Services+with+Access+codes/Important+security+information/760244.html>
- NORDEL (2004). *Nordel Yearbook 2004*. Available at:
<http://www.nordel.org/content/Default.asp?PageID=213>
- NSHS (2002). *The National Strategy for Homeland Security*. Office of Homeland Security. The White House. July 2002.
- NSPPCI/KA (2003). *The National Strategy for Physical Protection of Critical Infrastructures and Key Assets*. The White House. February 2003.
- NSSC (2003). *The National Strategy to Secure Cyberspace*. The White House, Washington. February 2003.
- ODP (2005). *ODP Information Bulletin No. 147* January 19, 2005. Available at:
<http://www.ojp.usdoj.gov/odp/docs/info147.htm>
- OECD (2006). *OECD Studies in Risk Management Denmark. Assessing societal risks and vulnerabilities*. OECD Studies in Risk Management.
- OVERILL, R. E. (2001). Information Warfare: Battles in Cyberspace. *Computing & Control Engineering Journal*. Vol. 12, Issue 3, pp. 125-128.

- OVILIUS, MAGNUS (2007a). Senior Administrator, Directorate General Justice, Freedom and Security, European Commission, response by *e-mail* 21 Feb 2007 to Piia Nikula.
- OVILIUS, MAGNUS (2007b). *A European Programme for Critical Infrastructure Protection EPCIP*. Head of Sector Preparedness and Crisis Management European Commission, DG Justice Freedom and Security. Powerpoint presentation, June 2007.
- PAKA, W. (2007). Deployment, toxicity and influence on the environment and other issues connected with sea-dumped chemical weapons. In: *Proceedings of the International Conference on Environmental Threats to the Baltic Sea held in Warsaw Sheraton Hotel*, 28 May 2007. Available at: www.senat.gov.pl/k6/agenda/seminar/070528e/indexer.htm
- PARFOMAK W. PAUL (2005). *Vulnerability of Concentrated critical Infrastructure: Background and Policy Options*. CRS Report for Congress. Received through the CRS Web. Order Code RL33206. Congressional Research Service. The Library of Congress.
- PARTANEN J., J. LASSILA, T. KAIPIA, M. MATIKAINEN, P. JÄRVENTAUSTA, P. VERHO, A. MÄKINEN, K. KIVIKKO, J. PYLVÄNÄINEN AND V-P. NURMI (2006). *Sähköverkkoon soveltuvat toimitusvarmuuskriteerit ja niiden raja-arvot sekä sähkönjakelun toimitusvarmuudelle asetettavien toiminnallisten tavoitteiden kustannusvaikutukset*. (s.I.): Lappeenranta University of Technology and Tampere University of Technology.
- PCCIP (1997). *President's Commission on Critical Infrastructure Protection Critical Foundations. Protecting America's Infrastructures*.
- PDD (1998). *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (PDD 63)*. May 22, 1998. WHITE PAPER.
- POLICE MINISTRY OF INTERIOR (2007). *Visit of the representatives of the Lithuanian Ministry of Interior and the Police to Poland*. Available at: <http://www.mswia.gov.pl/portal/en/1/287/>
- POLLARD, C. (2005). Telecom Fraud: The Cost of Doing Nothing Just Went Up. *Network Security*, pp. 17-19.
- POULSEN, K. (2004). FBI Busts Alleged DDoS Mafia, *Security Focus*, 28 August 2004. Available at: www.securityfocus.com/news/9411
- POULSEN, K. (2006). The Backhoe: A Real Cyberthreat. *Wired*. Available at: <http://www.wired.com/science/discoveries/news/2006/01/70040>
- PROBLEMSTUDIE: RISIKEN IN DEUTSCHLAND (2005a). Gefahrenpotentiale und Gefahrenprävention für Staat, Wirtschaft und Gesellschaft aus Sicht des Bevölkerungsschutzes - Auszug - Teil 1. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe - Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ), im Auftrag des Bundesministeriums des Innern. August 2005.

- PROBLEMSTUDIE: RISIKEN IN DEUTSCHLAND (2005b). Gefahrenpotentiale und Gefahrenprävention für Staat, Wirtschaft und Gesellschaft aus Sicht des Bevölkerungsschutzes - Auszug - Teil 2. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe - Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ), im Auftrag des Bundesministeriums des Innern. August 2005.
- PROTECTION OF CRITICAL INFRASTRUCTURES AND CRITICAL SOCIETAL FUNCTIONS IN NORWAY (2006). *Protection of critical infrastructures and critical societal functions in Norway*. Report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006. English Summary 1st of July 2006.
- PURSIAINEN, C. (2007). Who is afraid of the NEGP – and why? *Journal of Nordregio* No. 2 June Volume 7 2007, pp. 22-23, Stockholm.
- RÄDDNINGSVÄRKET (2001). The Effect of Common Oil Spill Projects and the Need for Future Activities. Report from Workshop in Karlskrona, August 2001. Available at:
<http://www.srv.se/upload/R%C3%A4ddningstj%C3%A4nst/olja/publikationer/The%20Effect%20of%20Common%20Oil%20Spill%20Projects.PDF>
- RANKILA, M. (2007). Vesivarat. In: *Vesitalouden verkkokirja (In Finnish)*. Water Resources Engineering, Helsinki University of Technology. Available at:
<http://www.water.tkk.fi/wr/kurssit/verkkokirja/sisallys.html>
- RANTANEN, H. (2003). *Managing Emergency Response with the Help of Information Technology. A Feasibility Study in the Finnish Perspective*. Licentiate Thesis, University of Kuopio.
- RANTANEN, M. (2007). Virtual Harassment, But For Real. *Helsingin Sanomat* Available at:
www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868
- RAUSCHER, K. F. ET AL. (2006). Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security. *Bell Labs Technical Journal*. Vol. 11, No. 3, pp. 73-81.
- REGIONAL DISASTER RESILIENCE (2006). *Regional Disaster Resilience: A Guide for Developing an Action Plan*. The American Society of Civil Engineers/ The Infrastructure Security Partnership (TISP), June 2006.
- REINEMA, R. (2004). *ACIP Analysis & Assessment for Critical Infrastructure Protection*. Security Management – Part 3: Critical Infrastructure Protection, Malta Lecture, Malta. January 29-30 2004 Available at:
http://www.csm.org.mt/pdf/Fraunhofer/SecMngmt_3_ACIP_Final.pdf
- RINALDI, STEVEN M., JAMES P. PEERBOOM AND TERRENCE K. KELLY (2001). *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*. IEEE Control Systems Magazine. December 2001.

- RISK ASSESSMENT AND PRIORIZATION (2003). *Volpe journal* 2003. John A. Volpe National Transportation Systems Center.
- RISK- OCH SÅRBARHETSANALYSER (2005) *Risk- och sårbarhetsanalyser år 2005. En analys per samverkansområde av myndigheternas risk- och sårbarhetsanalyser med koppling till Krisberedskapsmyndighetens årliga uppföljning*. Krisberedskapsmyndigheten, Stockholm. 2006-08-31, Dnr 0222/2006.
- ROBINSON C. PAUL, JOHN B. WOODARD, SAMUEL G. VARNADO (1998). How vulnerable is our interlinked Infrastructure? Critical Infrastructure: Interlinked and Vulnerable. *Issues in Science and Technology Online*.
- ROZENBLIT, M. (2000). *Security for Telecommunications Network Management*. New Jersey: IEEE Press.
- RYTKÖNEN, JORMA AND GENNADY SEMANOV (2005). *Baltic Oil Spill safety – recent trends of marine oil transportation in the Baltic Sea*, Presentation at the Oil Spill Detection and Combating in Ports` Workshop. 7 -9 June 2005. BOSS project /EU/Tacis. St. Petersburg.
- RYTKÖNEN, JORMA (2006). *Latest development of oil and chemical transportations on the Baltic Sea*. Presentation at the Conference on Dangerous Goods Transportation. St. Petersburg, Russia, 26 Oct. 2006.
- RYTKÖNEN, JORMA (2007): *Increasing Maritime Transport, Impacts on Maritime Safety*. Presentation at the International Seminar on Baltic Maritime Safety Co-operation and Oil Spill Management Personnel Training. St. Petersburg, Russia, 5.– 6. June 2007. Available at: http://www.vtt.fi/inf/julkaisut/muut/2007/Increasing_maritime_transport_2007.pdf
- SAARNISTO, M. AND SAARINEN, T. (2001). Deglaciation chronology of the Scandinavian Ice Sheet from the Lake Onega basin to the Salpausselkä end moraines. In: Thiede, J. [et al.] (eds.) *The Late Quaternary stratigraphy and environments of northern Eurasia and the adjacent Arctic seas - new contributions from QUEEN: selected papers from the annual QUEEN workshops held in Øystese, Norway, April 1999, and in Lund, Sweden, April 2000*. Global and Planetary Change 31 (1 - 4), 387 - 405.
- SALONEN, V-P., M. ERONEN AND M. SAARNISTO (2002). *Käytännön maaperägeologia*. Otava.
- SCHMIDT-THOMÉ, PHILIPP, ED. (2006a). *Sea Level Change Affecting the Spatial Development of the Baltic Sea Region*. Geological Survey of Finland. Special Paper 41. Geological Survey of Finland, Espoo.
- SCHMIDT-THOMÉ, P., (2006b). Thesis: *Integration of natural hazards, risk and climate change into spatial planning practices*. Geological Survey of Finland, Espoo.
- SCHULMAN, PAUL R. AND EMERY ROE (2007). *Defining Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures*.

- Contingencies and Crisis Management*, Volume 15 Number 1, March 2007, pp. 42-49.
- SCHUTZ KRITISCHER INFRASTRUKTUREN – BASISSCHUTZKONZEPT (2005). Empfehlungen für Unternehmen. Bundesministerium des Innern, August 2005.
- SCIENCE AND TECHNOLOGY COMMITTEE OF THE HOUSE OF LORDS (BRITAIN) (2007). *Personal Internet Security*. Vol. 1 (HL Paper 165-I), 5th Report of Session 2006–07.
- SEMA (2007). *Critical Societal Functions*. Swedish Emergency Management Agency. March 2007.
- SHELLEY, L. (2003). Organized Crime, Terrorism and Cybercrime. In: BRYDEN, A. AND FLURI, P., ED, *Security Sector Reform: Institutions, Society and Good Governance* Baden-Baden: Nomos Verlagsgesellschaft.
- SHERWOOD, J. ET AL., (2005). *Enterprise Security Architecture: A Business-Driven Approach*. CMP Books.
- SHIREY, R. (2000). *Internet Security Glossary*. IETF RFC 2828 Available at: <http://www.ietf.org/rfc/rfc2828.txt>
- SIAU, K. AND TAN, X. (2005). Technical Communication in Information Systems Development: The Use of Cognitive Mapping. *IEEE Transactions on Professional Communications* Vol. 48, No. 3, pp. 269-284.
- SILANDER, J. ET AL. (2006). *Climate change adaptation for hydrology and water resources – FINADAPT*. Working Paper 6. Finnish Environment Institute Mimeographs 336, Helsinki, 54 p. Available at: <http://www.ymparisto.fi/default.asp?contentid=194115&lan=en>
- SMART ECONOMIST (2005). The Dot-Com Bubble Revisited. *Smart Economist*. Available at: <http://www.smarteconomist.com/insight/68>
- SOLBERG, K. (2007). Tens of Thousands Risk ID Theft. *Aftenposten*. 10 August 2007.
- SONNINEN, SANNA, MAARIA NUUTINEN AND TONY ROSQVIST (2006). *Development Process of the Gulf of Finland Mandatory Ship Reporting System. Reflections on the Methods*. VTT Publications 614. Otamedia, Espoo.
- SOSIAALI- JA TERVEYSMINISTERIÖ (2000). Sosiaali- ja terveystieteiden ministeriö. *Asetus talousveden laatuvaatimuksista ja valvontatutkimuksista*, nro. 461. Helsingissä 19.5.2000.
- SOSIAALI- JA TERVEYSMINISTERIÖ (2001). *Päätös pienten yksiköiden talousveden laatuvaatimuksista ja valvontatutkimuksista*, nro. 401. Helsingissä 17.5.2001.
- SOVERI, J., R. MÄKINEN AND K. PELTONEN (2000). *Pohjaveden korkeuden ja laadun vaihteluista Suomessa 1975-1999* (Changes in groundwater levels and quality in Finland in 1975-1999, in Finnish with English summary). Finnish Environment Institute. Report 420.

- SSFVS (2006). *The Strategy for Securing the Functions Vital to Society*. The Government of Finland. Government Resolution 23.11.2006. Available (in English) at: www.defmin.fi/
- STALLINGS, W. (2003). *Network Security Essentials: Applications and Standards*. New Jersey: Prentice Hall.
- STERN (2006). *The Economics of Climate Change*. Available at: <http://www.hm-treasury.gov.uk>
- SUTER, M. (2007). *A Generic National Framework for Critical Information Infrastructure Protection (CIIP)*. Submitted to ITU-D Study Group Question 22/1, June 2007.
- SVERIGES BEREDSKAP MOT NÄTANGREPP (2007). Informations säkerhetsenheten, Gruppen för omvärldsanalys, Krisberedskapsmyndigheten 30.11.2007, Stockholm. Available at: <http://www.krisberedskapsmyndigheten.se/upload/15926/sveriges-beredskap-mot-natangrepp.pdf>
- SWEDISH MARITIME ADMINISTRATION (2003). *Action plan for Maritime Transport in the Baltic Sea Region. Review 2003*. Available at: <http://www.sjofartsverket.se/upload/1486/ActionPlan-review.pdf>
- SWEDISH RESCUE SERVICES AGENCY (2005). *Stormen Gudruns påverkan på räddningstjänstens tekniska infrastruktur*. Karlstad: Räddningsverket
- SYKE - FINNISH ENVIRONMENT INSTITUTE, (2007). *Groundwater resources*. Available at: <http://www.ymparisto.fi/default.asp?contentid=67942&lan=en>
- TAFAZOLLI, R. ED. (2005). *Technologies for the Wireless Future: Wireless World Research Forum (WWRF)*. Wiley: Chichester.
- TETRA MOU ASSOCIATION (2004). *Push To Talk over Cellular (PoC) and Professional Mobile Radio (PMR)* , May 2004.
- THREATS AND RISKS REPORT (2005). Special Feature 2005:11. Swedish Emergency Management Agency, Stockholm.
- THOMAS, R., AND J. MARTIN (2006). The Underground Economy: Priceless. *Login*, Vol. 31, No. 6, December 2006. Available at: <http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf> .
- TRAUNMÜLLER, R. AND K. LENK, EDS. (2002). Lecture Notes In Computer Science, *Proceedings of the First International Conference on Electronic Government*. Vol. 2456, pp. 37-44, 2002.
- TUOMAALA P. (2002). *Tulisijan ja lämmitys- ja ilmanvaihtojärjestelmien yhteiskäyttö (s.I.)*: VTT Technical Research Centre of Finland.
- TURUN SANOMAT EDITORIAL. (2007). Essential Networks Should be Protected from Malicious Attacks. *Turun Sanomat* 17 May 2007; English version of article compiled by SALLINEN, S., for *Helsinki Times*, 23-29 May 2007.

- U.S. DHA (2006). *Privacy Impact Assessment for the Critical Infrastructure Warning Information Network*. Department of Homeland Security. January 7, 2006.
- UITP (2006). *UITP International Association of Public Transport. Position on Green Paper COM(2005) 576 concerning an European Programme for Critical Infrastructure Protection*. 7 March 2006.
- UNCLOS (1982). *United Nations Convention on the Law of the Sea*. Montego Bay, 1982.
- USGS (2000). *Groundwater resources for the future: Atlantic Coastal Zone, Fact Sheet 085-00*. Ground Water Department, U.S. Geological Survey. Homepage: <http://water.usgs.gov/ogw>
- VACCA, J. R. (2006). *Guide to Wireless Network Security*. Springer.
- VESTERBACKA, K. (2007). *Dose Rate Monitoring Network Utilizing VIRVE*. Presentation at VIRVE Day 2007. Helsinki. 1 March 2007.
- VIITANEN T. (2002). *Myrskyn aiheuttamat yhteiskunnalliset häiriöt*. Pelastusosasto, Sisäasiainministeriö.
- VILPPUNEN, H. (2005). *The Role of TETRA in a Holistic Homeland Security Solution*. Presentation at 1st Argentinian TETRA Conference, Buenos Aires. 22 September 2005. Available at: http://www.tetramou.com/uploadedFiles/Files/Presentations/Arg05_HVilppunen_TETRA%20in%20Homeland%20Security.ppt
- VOLLAN, A. (2006). RAKEL boss Nils Svartz: - More co-operation across national borders with nationwide network. *The Directorate for Emergency Communication*, 6 May 2006; Available at: <http://www.dinkom.no/default.asp?pubid=904&sub=1&pub=1&labb=uk>
- WASSENAAR ARRANGEMENT (2007). *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. Available at: <http://www.wassenaar.org/index.html>
- WEHNER, R. (2006). How secure is your computer? 'Honey pot' experiment shows unprotected Windows SP 1 at risk. *The Denver Post*. 28 February 2006.
- WEIJNEN, M. (2007). Next Generation Infrastructures: Facing the Complexity Challenge. *European CIIP Newsletter* Vol. 3, No. 1, pp. 16-20.
- WILSON, CLAY (2006). Terrorist Capabilities for Cyber-attack. In: MYRIAM DUNN AND VICTOR MAUER, EDS. (2006). *International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects*. Series editors Andreas Wenger and Victor Mauer. ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich, pp.71-88.
- WWF FINLAND (2007a). *WWF esittää kuuden kohdan reseptiä tehokkaampaan öljyonnettomuuden ehkäisyyn*. Available at: http://www.wwf.fi/tiedotus/tiedotteet/tiedotteet_2007/esittaa_kuuden_kohdan.html

- WWF FINLAND (2007b). *Matkustajalaivojen jatevedet*. Available at http://www.wwf.fi/ymparisto/meret_jarvet/itameri/matkustajalaivojen_jatevedet.html YLE NEWS 1.6.2007.
- YOO, I. (2005). *Program Security*. Lecture notes, University of Fribourg. 10 November 2005.
- ZDF (2005). Abenteuer Wissen: Tückische Fundstücke. Vermeintlicher Bernstein entpuppt sich als gefährliche Chemikalie. Zweites deutsches Fernsehen, *TV programme* 19.10.2005 Available at: <http://www.zdf.de/ZDFde/inhalt/29/0,1872,2386973,00.html>.
- ZONE-H. (2007). *Examples of defaced websites*. Available at: <http://zone-h.org/>

Christer Pursiainen (ed.) with the assistance of Patrick Lindblom and Per Francke

Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection

Nordregio Report 2007:5

Critical infrastructures are such systems, which are essential for the maintenance of vital societal functions, including the supply chain, health, safety, security, economic and social well-being of people. With the European Commission Green Paper, published in November 2005, and Proposal for a Directive of the Council from December 2006, a European dimension has emerged in the field of critical infrastructure protection.

This development towards a more integrated European critical infrastructure protection is a clear challenge for the national models and strategies, which differ from country to country. Another challenge is the regional dimension. How, in the context of the EU-27, would it be possible to take into account the particular regional cross-border effects of critical infrastructure vulnerabilities as well as the specific features of European sub-regions?

This study discusses these issues from the specific perspective of the Baltic Sea Region. While it draws a general picture of critical infrastructure protection in this context, it initiates discussion about the issue of whether a regional level of critical infrastructure protection would be needed as an intermediate level between the strategies of national governments and the European Union.

The study also offers detailed case studies in such fields as electricity, information and communication technology, oil transportation and maritime safety, gas pipelines, and water. As a whole the study provides information, arguments and proposals that hopefully will lead to even more vigorous debates and discussion on critical infrastructure protection in Europe and elsewhere, and contributes to much needed awareness-raising in this field.



Nordregio
P.O. Box 1658
SE-111 86 Stockholm, Sweden
nordregio@nordregio.se
www.nordregio.se
www.norden.org



Project part-financed by the European Union within the European Programme for Critical Infrastructure Protection



Nordic Council of Ministers

ISSN 1403-2503

ISBN 978-91-89332-66-9