JYU DISSERTATIONS 173

Aarne Hummelholm

Cyber Security and Energy Efficiency in the Infrastructures of Smart Societies

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 173

Aarne Hummelholm

Cyber Security and Energy Efficiency in the Infrastructures of Smart Societies

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 3
joulukuun 17 päivänä 2019 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 3, on December 17, 2019 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2019

Editors
Timo Männikkö
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-8004-7

ISBN 978-951-39-8004-7 (PDF)
URN:ISBN:978-951-39-8004-7
ISSN 2489-9003

ABSTRACT

Hummelholm, Aarne
Cyber Security and Energy Efficiency in the Infrastructures of Smart Societies
Jyväskylä: University of Jyväskylä, 2019, 175 p.
(JYU Dissertations
ISSN 2489-9003; 173)
ISBN 978-951-39-8004-7

This dissertation examines architectures in smart cities and smart societies and also analyses the communications systems security, cyber security and energy efficiency of infrastructures, digital information systems and services, and underwater optical cable systems. The study also develops models for calculating the probabilities of cyber threats to these entities. This study first examines how digitalisation affects society and the daily lives of its citizens, its various services, and the environment. Our societies' digital services even now are available anytime and anywhere, in real time. The changes brought about by digitalisation of the various services available in our daily lives have a large impact on society and the lives of its citizens. To take full advantage of the services offered by digitalisation, people must be able to use secure smart devices and communication systems to use the services. However, there is a need to examine how we can improve and provide these services securely, anytime and anywhere in real time, and determine how the current services will work with future information systems and service structures. Security and cyber security threats must be taken into account when providing and developing these services because these services and infrastructures are subject to ubiquitous security and cyber security threats on a daily basis. Natural threats and risks also have an occasional impact on the availability and continuity of services, especially in the Arctic region. This dissertation introduces a single user device concept designed to reduce and prevent the impact of potential network threats and cyber-attacks in future environments and services. As the number of available services and the energy consumption of different systems increase exponentially, the volumes of harmful greenhouse gases that are often transported directly into the air also increase exponentially. More attention must therefore be given to the root causes of climate change and, in particular, to services with a high energy consumption. Despite discussing digitalisation and its importance in our services, the effects of digitalisation on the growth of energy consumption and its consequences are not sufficiently taken into account in our societies. Thus, we consider whether it is possible to reduce the energy consumption of services and thereby reduce greenhouse gas emissions. When building new ecosystems or improving existing solutions and structures, cost-effectiveness needs to be considered and improved to improve operational efficiency across all sectors.

Keywords: smart cities, smart society, energy consumptions, risks, threats, cyber-attacks, climate change, greenhouse gases.

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Hummelholm, Aarne
Kyberturvallisuus ja energiatehokkuus äly-yhteiskunnan infrastruktuureissa
Jyväskylä: University of Jyväskylä, 2019, 175 p.
(JYU Dissertations
ISSN 2489-9003; 173)
ISBN 978-951-39-8004-7

Väitöskirjassa tutkitaan älykaupunkien ja äly-yhteiskuntien sekä arktisen alueen arkkitehtuureja. Tutkimuksessa analysoidaan turvallisuus-, kyberturvallisuus- ja energiatehokkuuskysymyksiä infrastruktuureista, digitaalisista tietojärjestelmistä ja palveluista, sekä merenalaisista optisista kaapelijärjestelmistä. Lisäksi esitetään malleja näihin kokonaisuuksiin kohdistuvien kyberuhkien todennäköisyyksien laskelmista varten. Tutkimusten lähtökohtana on tarkastella, miten digitalisaatio vaikuttaa yhteiskunnan ja sen kansalaisten jokapäiväiseen elämään, sen eri palveluihin ja miten sen mukanaan tuomat muutokset näkyvät jokapäiväisessä elämässämme ja ympäristössämme. Yhteiskunnan digitaaliset palveluthan ovat saatavilla reaaliaikaisesti missä ja milloin tahansa. Kaikkien digitalisoinnin tarjoamien mahdollisuuksien hyödyntämiseksi on pystyttävä käyttämään turvallisia älylaitteita ja viestintäjärjestelmiä kaikkien meille tarjottavien palveluiden kanssa. On tarkasteltava kaikkia niitä mahdollisuuksia, joilla voimme parantaa ihmisten päivittäisiä palveluita ja kuinka tarjota näitä palveluita reaaliajassa ja turvallisesti, missä ja milloin tahansa, ja kuinka nämä palvelut toimivat yhdessä nykyisten ja tulevien tietojärjestelmien ja palvelurakenteiden kanssa. Mutta tähän kehitykseen liittyvät samalla myös tietoturva- ja kyberturvallisuusuhkat, jotka on huomioitava palveluiden tarjoamisessa ja kehittämisessä. Näihin palveluihin ja infrastruktuureihin kohdistuu päivittäin kaikkialle ulottuvia turvallisuus- ja kyberturvallisuusuhkia. Luonnollisilla uhkilla ja riskeillä on myös satunnaisia vaikutuksia palveluiden saatavuuteen ja jatkuvuuteen etenkin arktisella alueella. Työssä esitellään myös yhden käyttäjän laitekonsepti, jonka tarkoituksena on parantaa käyttöturvallisuutta uusissa toimintaympäristöissä ja palveluissa. Kun saatavien palvelujen määrä kasvaa eksponentiaalisesti, samalla sen seurauksena eri järjestelmien tarvitsema energiankulutus kasvaa eksponentiaalisesti, mikä tarkoittaa myös sitä, että haitalliset kasvihuonekaasujen määrät kasvavat eksponentiaalisesti ja ne kulkeutuvat usein suoraan ilmaan. Meidän on kiinnitettävä huomattavasti enemmän huomiota ilmastonmuutoksen perussyihin ja erityisesti palveluihin, joiden energiankulutus on korkea.

Asiasanat: älykäs kaupunki, älykäs yhteiskunta, riskit, uhkat, kyber-hyökkäykset, ilmastomuutos, kasvihuonekaasut.

Author Aarne Hummelholm
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors Professor Dr Pekka Neittaanmäki
Faculty of Information Technology
University of Jyväskylä
Finland

Professor of Practice Dr Martti Lehto
Faculty of Information Technology
University of Jyväskylä
Finland

Professor Dr Timo Hämäläinen
Faculty of Information Technology
University of Jyväskylä
Finland

Docent Dr Tuija Kuusisto
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers Professor Dr Heikki Hämmäinen
Department of Communications and Networking
Aalto University
Helsinki
Finland

Prof. Janos Sztrik
Faculty of information,
University of Debrecen
Hungary

Opponent Docent Dr Rauno Pirinen
Finnish National Defence University
Helsinki
Finland

ACKNOWLEDGEMENTS

This thesis was carried out under the guidance of the Faculty of Information Technology of University of Jyväskylä between 2017 and 2019. During my professional career, I have had the opportunity to work in challenging professional roles and work environments, which has given me a wealth of knowledge and experience on a variety of issues. My experiences working with the Finnish Ministry of Finance and discussions concerning development work with representatives from the Ministries of Defence, Ministry of Foreign Affairs, Ministry of Interior, Ministry of Transport and Communications, Ministry of Justice, Ministry of Trade and Industry, Ministry of Social Affairs and Health as well as the Prime Minister's Office and Finnish Defence Forces have provided the perfect background for this thesis. My cooperation with various ministries made it possible for me to work with professionals in the field and to gain insights into communication system environments and services in real-life settings. I would like to thank the Finnish Communications Regulatory Authority and its professionals with whom I have discussed many critical issues related to communications systems and services in the auditing processes.

I am also grateful to all the professionals in academia who helped me along the way, making it possible to finish this doctoral thesis. My special thanks goes to my supervising professors, Pekka Neittaanmäki, Martti Lehto, Timo Hämäläinen and Tuija Kuusisto, for our discussions concerning many different topical issues and for the practical help they gave me during my work.

I would also like to thank Professors Janos Sztrik and Heikki Hämmäinen who reviewed my dissertation and I received instructions from them to my work.

In addition, I would like to thank Hanna-Leena Huttunen and Jenni Siermala for their research work, which opened new paths for my thesis. The inputs and ideas I received from them helped me to better understand the issues I was dealing with and allowed me to expand the horizon of my work. I extend my gratitude to them.

Finally, I would like to thank my lovely daughters, Heidi and Hanne, and their families for their support and encouragement. I am also indebted to my loving wife, Inkeri, for her patience and support throughout the duration of this work and for allowing me to share this process with her. I am also grateful to her sons, Olli and Heikki, and my sister-in-law, Ilona, who have helped me with proofreading and given me practical advice and ideas on language-related issues.

Jyväskylä 12.12.2019
Aarne Hummelholm

LIST OF ABBREVIATIONS

3GPP-5G	The 3rd Generation Partnership Project -5G
5G Norma	5G Novel Radio Multiservice Adaptative Network Architecture
5G-PPP	5G Infrastructure Public Private Partnership
AI	Artificial Intelligence
BER	Bit Error Ratio
BOL	Beginning of Life
CMDB	Configuration Management Database
CO_2	Carbon dioxide
COTDR	Coherent Optical Time Domain Reflectometer
CWDM	Coarse Wavelength Division Multiplexing
D2D	Device-to-Device
DCFL	Data Centre Functions Slicing
DWDM	Dense Wavelength Division Multiplexing
EA	Enterprise Architecture
ECCWS	European Conference on Cyber Warfare and Security
EDGE	EDGE computing
EMC	Electromagnetic Compatibility
EMP	Electromagnetic pulse
EOL	End of Life
EPA	The Environmental Protection Agency
ESB	Enterprise Service Bus, IBM-system
EU-GDPR	European Union - The General Data Protection Regulation
EU-MDR	European Union - The Medical Devices Regulation
EU-NIS	European Union - Concerning measures for a high common level of security of network and information systems across the Union
FW	Firewall
GW	Gateway
HAPS	High Altitude Platform for Services
Horizon (EU)	EU Research and Innovation programme
HPM	High Power Microwave weapon
ICT	Information and Communication Technology
IEEE	The Institute of Electrical and Electronics Engineers
IIMP	Intelligent Information Management Platform
IMT	International Mobile Telecommunication
IPsecVPN	Internet Protocol security Virtual Private Network
LANs	Local Area Networks
IDS	Intrusion Detection systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPS	Intrusion Protection Systems
ITU-T	International Telecommunication Union
JHS	The Public Administration Recommendations - JHS recommendations
JUFO	Julkaisu Foorumi, Publication Forum

KATAKRI	National Audit Guide
M2M	Machine-to-Machine
MEC	Mobile Edge Computing
Metis (EU)	METIS 2020, Mobile and wireless communications Enablers for the Twenty-twenty Information Society 5G
MPLS	Multiprotocol Label Switching
NFV	Network Function Virtualisation
N-ISDN	Narrowband Integrated Services Digital Network
NMT	Nordic Mobile Telephone
NOC	Network Operation Centre
OFA	Optical Fiber Amplifier
OTDR	Optical Time Domain Reflectometer
PDG	Polarisation-Dependent Gain
PDL	Polarisation-Dependent Loss
PeAN	Personal Access Node
PMD	Polarisation Mode Dispersion
Q	Quality factor
QFD	Quality Function Deployment
RTT	Round Trip Time
SAN	Service Area Network
SDDC	Software Defined Data Centres
SDN	Software Defined Network
SIEM	Security and Information Event Management
SSLVPN	Secure Sockets Layer Virtual Private Network
SOC	Security Operation Centre
STI	The level of protection, Top Secret
STII	The level of protection, Secret
STIII	The level of protection, Confidential
STIV	The level of protection, Restricted
TAP	Traffic Analysis Points
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions
TTE	Terminal Transmission Equipment
V2X	Vehicle to Everything
VAHTI	The Government Information Security Management Board

LIST OF FIGURES

LIST OF TABLES

CONTENTS

LIST OF PUBLICATIONS

This dissertation is based on five publications and two patents.

PI Aarne Hummelholm, Cyber threat analysis in Smart City environments, ECCWS2018, 27-29 June 2018, Oslo, Norway, Published by Academic Conferences and Publishing International Limited, E-Book ISBN:978-1-911218-86-9, E Book ISSN:2048-8610. JUFO ID = 71915, JUFO level = 1.

PII Aarne Hummelholm, Undersea Optical Cable Network and Cyber Threats, ECCWS2019, 4-5 July 2019, Coimbra, Portugal, Published by Academic Conferences and Publishing International Limited, Book version ISBN: 978-1-912764-28-0, E Book ISSN:2048-8610. JUFO ID = 71915, JUFO level = 1.

PIII Heimir THORISSON[a], Fabrizio BAIARDI[b], Mirva SALMINEN[c], Rozelien Van ERDEGHEM[c], Rishikesh SAHAY[d], Bob PAQUIN[e], Charlee HEATH[f], Inna SKARGA-BANDUROVA[g], Mathieu BRANLAT[h], Aarne HUMMELHOLM[i], James H. LAMBERT[a], Igor LINKOV[j], Benjamin D. TRUMP[j], ´Cyber Security Challenges to Arctic Critical Infrastructures´,
[a] University of Virginia, [b] Università di Pisa, [c] University of Lapland, [d] MAN Energy Solutions, [e] Global Affairs Canada/Canadian International Arctic Centre, Oslo, [f] University of Ottawa, [g] East Ukrainian National University, [h] Sintef, [i] NATO Science for Peace and Security Series – D: Information and Communication Security, IOS Press, appear in 2019.

PIV Aarne Hummelholm, E-health systems in digital environments, ECCWS 2019, 4-5 July 2019Coimbra, Portugal, Published by Academic Conferences and Publishing International Limited, Book version ISBN: 978-1-912764-28-0, E Book ISSN:2048-8610. JUFO ID = 71915, JUFO level = 1.

PV Aarne Hummelholm, Threat characterization for various layers of infrastructure, in publications of Heimir THORISSON, Fabrizio BAIARDI, Mirva SALMINEN, Rozelien Van ERDEGHEM, Rishikesh SAHAY, Bob PAQUIN, Charlee HEATH, Inna SKARGA-BANDUROVA, Mathieu BRANLAT, Aarne HUMMELHOLM, James H. LAMBERT, Igor LINKOV, Cyber Security Challenges to Arctic Critical Infrastructures, NATO Science for Peace and Security Series – D: Information and Communication Security, IOS Press, appear in 2019.

PVI Aarne Hummelholm, Kari Innala, Intelligent Base Station Comprising Functions Relevant to its Operation, Patent No.: US 8,606,320 B2, Date of Patent: Dec. 10, 2013.

PVII Aarne Hummelholm, Communications Network, Systems and Device, Publication No: 119900, Publication Date: 30. 4.2009.

Publications I - V were not included as appendices because this type of monograph dissertation deals with the subject more extensively than do publications I - V and the essential content of these publications is presented in this work. Patents VI - VII were also not included as appendices because their contents are included in Chapters 5 and 6. This dissertation used only public information.

AUTHOR'S CONTRIBUTION TO THE ARTICLES

The author wrote publications I – V and VII completely independently based on his research and work in different positions at the Ministry of Finance and the Finnish Defence Forces. The author wrote patent publication VI with Kari Innala.

PI The author presented the research contained in this publication about cyber threats in smart city environments at the ECCWS 2018 conference on 27-29 June 2018 in Oslo, Norway.

PII This publication is based on the author's research into undersea optical cable networks and cyber threats in the Arctic connect project and cyber security control, the ARCY projects, prepared for the Faculty of Information Technology, University of Jyvaskyla, Finland, which the author presented at the ECCWS 2019 conference on 4-5 July 2019 in Coimbra, Portugal.

PIII This publication is based on the Governance for Cyber Security and Resilience in the Arctic, 2019 NATO conference held on 27-30 January 2019, in Rovaniemi, Finland, and on discussions held in working groups. All writers of Cyber Security Challenges to Arctic Critical Infrastructures are involved in write this part.

PIV This publication is based on the author's research and analysis of threat characterization in e-health systems in digital environments, in future hospitals in Oulu and in future homes in Kajaani, which the author presented at the ECCWS 2019 conference on 4-5 July 2019 in Coimbra, Portugal.

- The author's contribution on 'E-health Systems in Digital Environments' was the winner of Best PhD Paper and Presentation award at ECCWS 2019 (the 18th European Conference on Cyber Warfare and Security 2019) on 4-5 July 2019 in Coimbra, Portugal.

PV This publication was based on the author's research Threat characterization for various layers of infrastructure in the Arctic region, 2019.

PVI This patent publication is based on research in the wireless communications field. The study examines the way in which wireless technology works in smart cities environments and determines what must be done in a new energy efficient way. The object of the invention is a mobile base station network and the base station used therein. According to the invention, an intelligent base station is developed. Each base station functions independently and comprises all the important functions relevant to its operation including the data transmission, transfer and control functions and used channels exchanges. The advantage of an intelligent base station is that it has a limited number of necessary functions, but expansion features, such as outer interfaces, can easily be added.

PVII This patent examines how to improve wireless communications networks and ameliorate their usability and the quality of services offered. The invention concerns a novel mobile communication network and network topology, systems and device, and presents a method for designing and optimising the network. According to the invention, instead of using a single directional antenna and / or one base station, the coverage area and services use a number of directional antennas and / or base stations for the needs of the user terminal, from which user terminal selects the best connection to its service.

OUTLINE OF THESIS

This thesis consists of six chapters based on five publications (PI – PV) and two patents information.

Chapter 1 presents the introduction.
Chapter 2 discusses cyber threats in smart city environments.
Chapter 3 deals with undersea optical cable network and cyber threats.
Chapter 4 discusses threat characterisation for various layers of infrastructure.
Chapter 5 addresses È-health systems in digital environments.
Chapter 6 presents a solution model for a new type of smart devices and a new network concept based on two patent papers.
Chapter 7 concludes the dissertation.
Two appendices are shown on the last pages in this thesis.

CHAPTER 1. INTRODUCTION

1.1 Outline of challenges of the smart cities and of the research areas

This dissertation examines future societies and smart cities, and their infrastructures, telecommunications solutions and data centre needs. This study also discusses future societal changes and services provided to people and the associated cyber threats and security threats. Initially, the study examines the services of smart cities and their distribution into different service segments. Additionally, a set of smart cities in one region in one country, in one continent and in the Arctic region is described. The study then discusses how the various continents are interconnected to form one global entity (Figure 1; PI – PIII and PV).

The study uses a completely new approach, presented in chapter 2, and thus divides the structures of society into six segments; basic infrastructures, energy, mobility, buildings and homes, public services, communications and IoT services. One review in chapter 2 (Figure 5), examines the drivers of change that will impact future smart cities and smart societies in one country, across continents and in the Arctic. Another review in chapter 2 (Figure 6), illustrates the significance of the EU directives, laws, regulations, standards, and national requirements and guidelines in chapter 2.

The approach is different to, for example, the way the International Electrotechnical Commission (IEC) presented the structures and services of smart cities (IEC, 2014). The IEC divided the future urban environment into five segments: Energy, Mobility, Buildings and Homes, Public Services and Water. Another method of smart city building is described in 'Smart Cities Readiness Guide', but the approach is also different to that used herein in this dissertation as it does not provide the necessary principles for its overall architecture (martCitiesCouncil, 2013).

One division is in the Beecham Research Sector Map, where the research institute has divided society into nine distinct research segments, with different functional backgrounds. This dissertation groups these segments in a new way that is more appropriate to the architecture work (Beecham, Beecham Research´s sector map). This study divides smart cities and smart societies into six segments to obtain a clear picture of the architectures and services of smart cities. This study applies Enterprise

Architecture Framework method and uses the QFD model to define the dependencies (QFD INSTITUDE) in different services and functions.

One research area in this dissertation is the submarine optical cable system which connects the intercontinental communication systems, which have been studied and analysed as a whole in PII, PIII and PV. The Arctic region has also been treated as a whole in PIII and PV. Communications satellites and the use of satellites for the other purposes have been studied (PIII) in this dissertation, using them for example in mobile communications systems in the Arctic region. Climate change issues have also been raised in relation to data centres, telecommunications networks and the services they offer, buildings and homes in the future, energy consumption, decreased energy consumption and renewable energy solutions.

This study examines the services these complex societal environments provide and researches the smaller functional entities and information systems they contain in terms of their dependencies, risks, vulnerabilities, cybersecurity threats and privacy concerns. The probability of potential threats or cyber-attacks has also been determined (PI -PV) (University of Cambridge) (Wang, Liu, 2014).

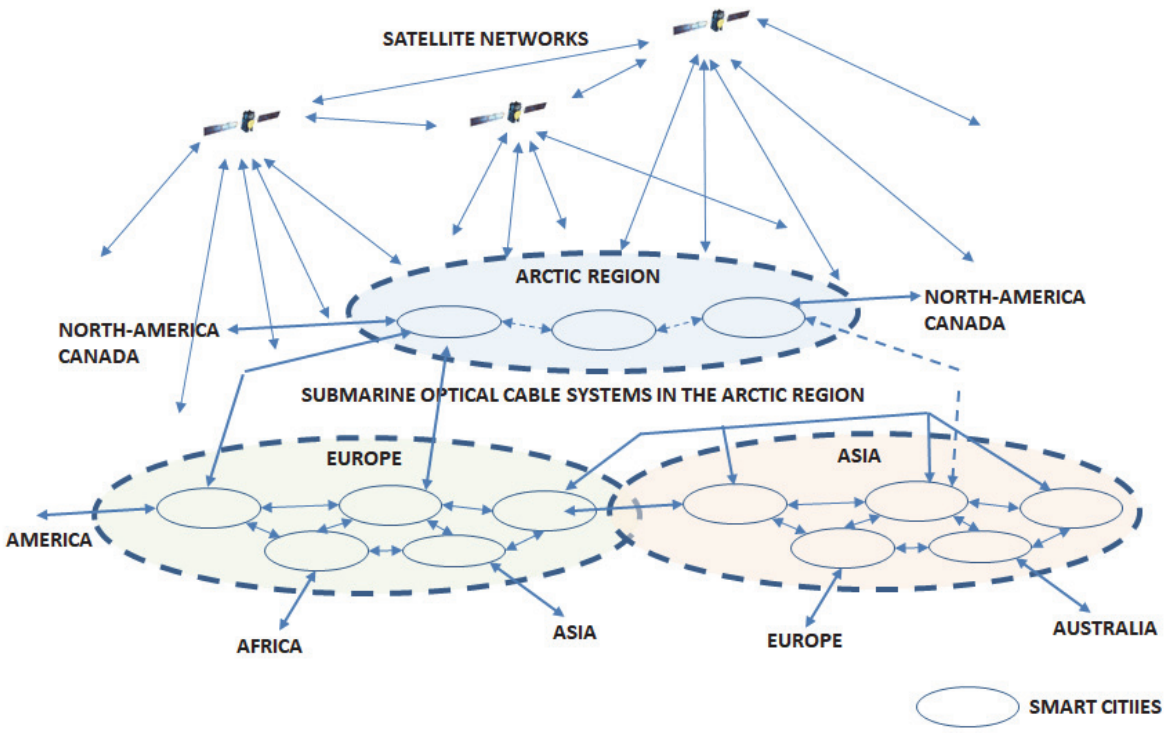
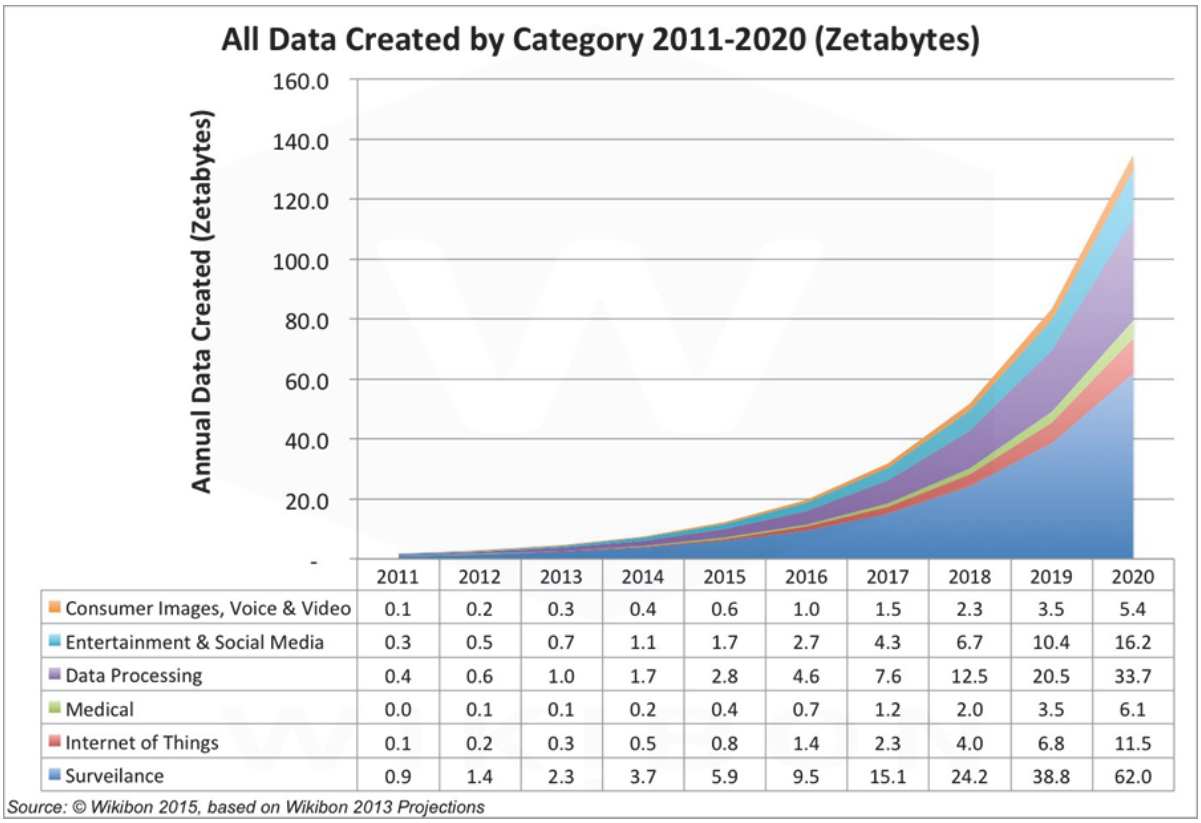


FIGURE 1. Smart cities, submarine optical cable systems and satellite systems of future smart societies in Europe, Asia and the Arctic region.

Smart societies worldwide produce huge amounts of information that need to be stored in data centres where it can be made available to citizens. However, such storage leads to a huge increase in energy demand by data centres, thus leading to a rapid increase in CO_2 and other greenhouse gas levels, which can be calculated using the Greenhouse Gas Equivalencies Calculator (EPA, 2007) (EPA, Greenhouse Gas Calculator).

Many estimates have been made about the growth of information worldwide; Figure 2 shows one of the latest estimates. The amount of information is growing exponentially, which means that the energy required by data centres is similarly increasing despite having already virtualised server and storage platforms in our data centres (Appendices 1 and 2). Virtualisation in this context means that many applications use the same processors and memory chip resources on servers and storage systems. Virtualization creates a simulated, or virtual, computing environment as opposed to a physical environment. Virtualization often includes computer-generated versions of hardware, operating systems and storage devices (based on the definition of Microsoft Azure).



	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Consumer Images, Voice & Video	0.1	0.2	0.3	0.4	0.6	1.0	1.5	2.3	3.5	5.4
Entertainment & Social Media	0.3	0.5	0.7	1.1	1.7	2.7	4.3	6.7	10.4	16.2
Data Processing	0.4	0.6	1.0	1.7	2.8	4.6	7.6	12.5	20.5	33.7
Medical	0.0	0.1	0.1	0.2	0.4	0.7	1.2	2.0	3.5	6.1
Internet of Things	0.1	0.2	0.3	0.5	0.8	1.4	2.3	4.0	6.8	11.5
Surveilance	0.9	1.4	2.3	3.7	5.9	9.5	15.1	24.2	38.8	62.0

Source: © Wikibon 2015, based on Wikibon 2013 Projections

FIGURE 2. All data created between 2011 and 2020 (Schmarzo, 2017).

An analysis of the above described continents' areas, countries, different segments and service entities in Figure 1 shows that considerable overall architectural work is needed to identify the environments we are working with and services being offered to the citizens, open EA Method (Dragon1-open) (JHS 179). State level organisations, government and ministerial departments, private organisations with big business sectors, national and international banks are the main targets of cyber attackers and hackers in our societies. Therefore, such organisations need to know the kinds of environments in which they are communicating with their customers and co-operating with other companies. The data growth shown in Figure 2 indicates that we need to have a lot of smart devices in use because many different types of information

systems and applications are needed to enable data growth (Figure 3). However, such data growth gives hackers and cyber attackers more opportunities and ways to attack our systems and services. They can use the same types of network and application analytics tools used by network and service operators to locate organisations, detect vulnerabilities in the devices and systems, search for specific devices and systems that are not properly protected, identify specific protocols in which they have found vulnerabilities and locate backdoors.

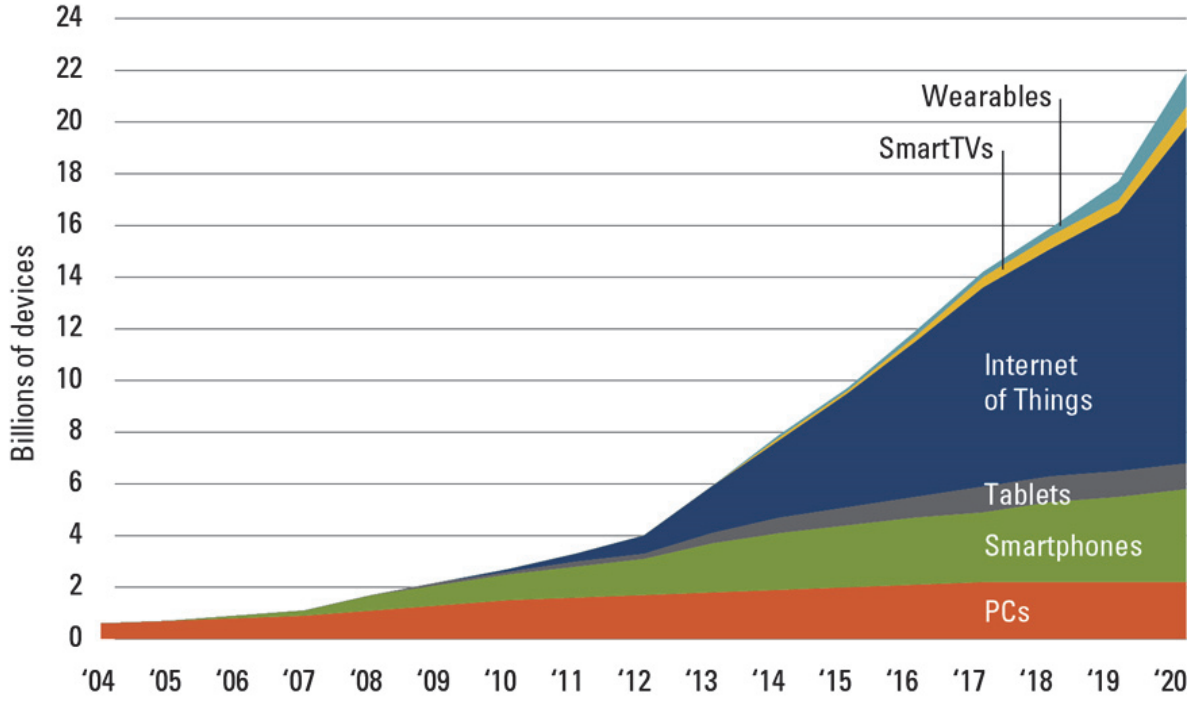


FIGURE 3. Forecast of global internet devices (Schmarzo, 2017).

When we look at the forecasts presented in Figures 2 and 3 and relate them to the development of the future smart cities and smart societies, we can see that considerable work is required to develop a vision, scenario work, strategy work and case study research, and to research the development and implementation of services. Such work will enable us to verify that those developments can move in the right direction, taking into account rapidly changing and evolving environments, use cases and societal changes in the day-to-day operations of citizens, as well as security and cyber security issues (see Figures 1 - 3).

Figures 1 - 3 show that virtualisation of all the devices used is not enough to reduce the energy consumption of the systems being currently used; other systems are also required (virtualization here means that many applications use the same processors and memory chip resources on servers and storage systems there). The use of our devices needs to be profiled according to needs and use, as well as data centre equipment, communication network equipment, mobile network equipment, users' devices, IoT devices and sensors (Appendices 1 and 2). The reason is that even if we use virtualized devices to save energy, they consume energy even though there is no need to

communicate or send information. Profiling here means that the energy consumed by the devices you use will monitor their actual daily use and, if necessary.

One quite new research area is zero-energy communications, which we can use, for example, in communications between IoT devices, sensors and users' devices.

Our living environments contain many broadcasting systems which require a lot of energy to work constantly. As people often watch TV programmes from their smart phones and devices, they do not need broadcasting systems, but rather mobile networks and the internet.

Even if we create a hybrid model of energy solutions for our smart environments that incorporate sun panels, wind generators and ground or geothermal heat systems, we must also consider the security and cyber-security issues because hackers and cyber-attackers can attack against our societies systems also through these new systems.

When performing virtualisation for data centre devices, communication devices and user terminals, we can use machine learning methods to manage and monitor the virtualised devices and environments. Network and data centres resources can be shared according to the needs of different operators and users and this way we can optimise the systems for a huge number of managed devices. When profiling the functionalities of the devices we use in our networks and data centres, we can also utilise machine learning intelligence for optimisation. Implementation of the zero-energy model in the use of different devices, data centres and communications systems should be investigated; it is also possible to exploit the potential of machine learning in this area.

When we have implemented virtualisations to all our information and communications systems and our smart devices, profiled their use and applied zero-energy possibilities to all of them, we can implement a 'Green Energy Communication Society' which uses information (Pazowski, 2015) (Kaushik, 2017) (Insights Success, 2019) (Oleg, 2011). The CO_2 emissions caused by flying are often discussed, but even before 2010, information and communications systems CO_2 emissions were higher than that of air traffic (Ellinger, Mikolajick, Wettwies, 2013). The Greenhouse Gas Equivalencies Calculator can be used to calculate the emission levels (EPA, Greenhouse Gas Calculator).

However, technical solutions for all new service environments are not yet in line with international standards. Their connections to telecommunications and service networks are very diverse and technically outdated solutions and new technologies are used simultaneously. Future information and communication systems need to be designed and adapted to work in this challenging business environment where security threats and cybercrime are constantly present. Each function has its own service and communication needs depending on the user group. These user groups include design and maintenance staff, financial management staff in different continents, telecom operators, service provider staff, virtual service providers and operators, administrative agents, citizens, manufacturers, banks. To date, no other technology apart from submarine cables systems has had such a strategic impact on our society while remaining so poorly understood by the general population. This means that submarine cables systems are a very tempting target for hackers and state actors who seek access to the submarine optical cables and networks connecting continents to each other.

This dissertation examines the impact of those in chapter 2, 3, 4 and 5 presented rapidly changing technological and non-technological factors on future smart city and smart society environments, submarine optical cable systems between continents and the Arctic region's infrastructures and services solutions. This study analyses cyber security in this rapidly changing environment to provide citizens with seamless services they can trust, irrespective of their time and location.

A special research area addresses the use of e-health systems in digital environments, future hospitals, smart home environments and wherever citizens travel because this issue is critical to citizens health now and in the future. The latest challenge for operating environments such as hospitals and homes involves providing seamless interconnections between heterogeneous telecommunication networks and new devices and systems. These systems include the Internet of Things (IoT), Device-to-Device (D2D), Machine-to-Machine (M2M) and Vehicle-to-Everything (V2X) systems, which have expanded into homes, office buildings, building automation systems, cars, and various control and energy systems (Beecham Research´s, Wearable Technology) (Beecham Research´s, World of Connected Device). Connecting devices to the internet and enabling their direct interaction saves money and time and improves efficiency. The integration process is accelerating at all levels of communications and in each region both horizontally and vertically, but the risk is also growing rapidly.

1.2 Research Questions

The research questions addressed in Chapter 2 are as follows:

RQ 1. Which tools can we develop for future communications and information architectures in smart cities?

> RQ 1.1. Which tools can we use to find dependencies between information systems, communications systems and different services?
> RQ 1.2. How can we implement services into a future society and its smart cities in such a way that citizens are able to use them safely in their everyday lives?
> RQ 1.3. How can we decrease our energy consumption in communications and information systems in smart cities and smart societies?
> RQ 1.4. What tools can we use for calculating the probabilities of cyber threats to smart cities and smart societies?

The research questions addressed in Chapter 3 are as follows:

RQ 2. What are the attack possibilities in submarine optical cable systems?

> RQ 2.1. How can we ensure that communication systems between continents are sufficiently secure to use them daily in our services

The following research questions are addressed in Chapter 4:

RQ 3. How we can provide services to the citizens of the Arctic region?

RQ 3.1. How can we implement a new type of energy efficient building, which also reduces CO_2 and greenhouse gas emissions in the Arctic region?

RQ 3.2. How can we implement new types of smart city and building architectures so that we can eliminate CO_2 and other greenhouse gases and save city space?

The research questions addressed in Chapter 5 are as follows:

RQ 4. How can we verify that information from patient sensors and IoT devices goes to the appropriate data centres that are used only by authorised people?

RQ 4.1. How can we verify e-health and other critical systems so that we can use them safely in the digital environment?

RQ 4.2. How well do the EU directives, national laws and recommendations guide our development and work to respond to patient information security, privacy and critical patient information?

The following research questions are addressed in Chapter 6:

RQ 5. Is it possible to implement D2D communication systems, for example, in hospital environments without any other communication network?

RQ 5.1. How we can implement a service network quickly and flexibly where it is needed without any other communication network?

The conclusions and summary are presented at the end of each chapter and the dissertation concludes with a summary of the studies and final conclusions.

1.3 Outline of thesis

This dissertation is based on five publications and material from two patents.

Chapter 1 introduces the dissertation issues, motivation and description of research and presents the cyber security issues and energy efficiencies in different smart society environments.

Chapter 2 presents the future smart cities and smart society environments discussed in this dissertation, outlines important functions in the various segments and architectures of our future environments, and describes the structures of the current society. This chapter also showcases future smart city infrastructures, services and smart city energy efficiency solutions. A cyber security threats analysis is also conducted for those environments.

Chapter 3 describes a solution to the delayed communication between Europe and Asia and analyses the security threats and natural threats in the areas where the submarine optical cable will be installed. This new submarine optical cable system will be installed between Europe, Finland, China and Japan crossing the Arctic see area.

Chapter 4 presents an overview of the Arctic region and its future communication service requirements for taking care of citizens' needs based on the service needs described by researchers at the University of Rovaniemi. This chapter also introduces the future communications systems required for citizens of the Arctic region including access networks and different types of satellite and other communications systems.

Chapter 5 presents e-health systems for use in future hospitals and home environments and for patients to use when performing their daily tasks.

Chapter 6 present and tests smart base station systems used for forming communication networks, systems and devices without any other networks present.

CHAPTER 2. CYBER THREAT ANALYSIS IN SMART CITY ENVIRONMENTS.

This chapter is based on publication PI entitled 'Cyber Threat Analysis in Smart City Environments' and additional materials from the author's works[1]. Appendices 1 and 2 show the energy efficiency values calculated for data centres and communications networks and they extend and deepens the content of the chapter.

2.1 Introduction

This chapter describes the methods used for assessing and analysing the cyber threats and risks affecting future society and smart cities and the everyday lives of people, and the author provides a model for risk and threat analysis (Figures 4 - 6). To detect cyber threats facing society and to define their impact on our everyday lives, we must first describe our future operating environment and highlight the key elements and structures (incl. solutions) affecting its functioning (Figures 4 - 6). The current societal structures are undergoing significant changes, in Figure 4, which affect the daily lives of all citizens in many ways. Figure 4 shows the structures and operating environments of societies which are subject to change. This future society produces huge amounts of information in digital form (see Figure 2), which means very high-power consumption by data centres (Appendix 1) to ensure every citizen has the information he or she needs at his or her disposal in real time, regardless of time and place (Limnell, Majewski, Salminen, 2014). As changes in social structures take place very quickly and affect the implementations and operating models, structures and people's everyday lives and working environments, the solutions currently in use are likely to be outdated in a few years' time. According to estimates, the telecommunications networks and mobile networks constructed in accordance with the currently used architectures cannot meet the needs of data transfer and storage beyond 2020 (EU FP7 ICT -317669- METIS). Broadband services require faster response times in order to work and the mobile network capacity needs to be increased from its existing solutions (Public Private Partnership (5G-PPP)). New types of services are coming into use and being offered in

[1] YETTS, The Security Strategy for Society,
https://www.defmin.fi/en/publications/strategy_documents/the_security_strategy_for_society

new ways. The current powerful digitalisation trend increases the range of services offered and facilitates their easier use. These developments also have a strong impact on the service chains of the provided services, including subcontractors with subcontracting chains, hardware solutions, service providers and operating models to every part of the service chain. To illustrate the complexity and future of smart city environments, infrastructures, and the connectivity and interoperability needs of different environments, this study divides the future smart city environment into different functional segments to identify the services offered (Figures 4 and 6).

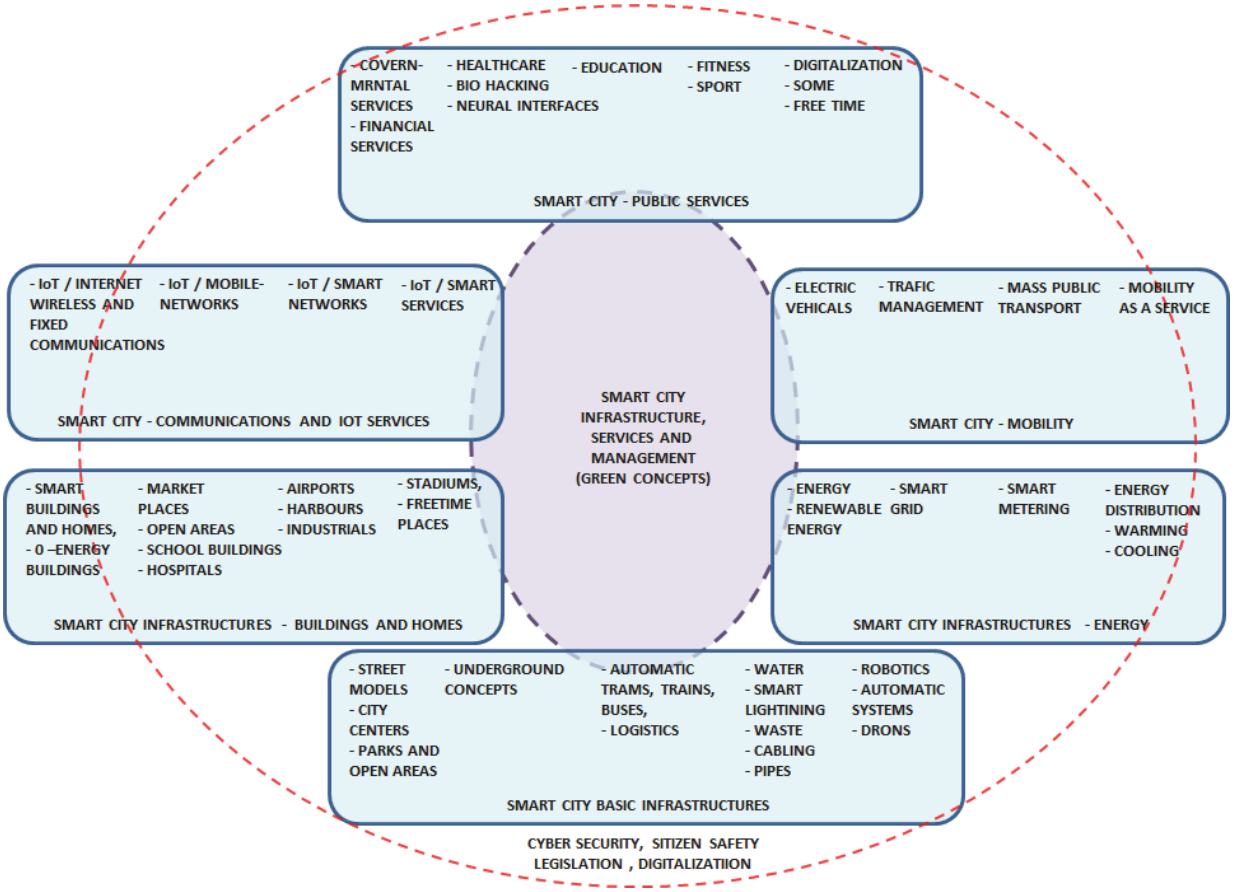


FIGURE 4. Smart city services in different service entities.

As a result of the developments described above, people and systems produce huge amounts of information that needs to be processed and stored. However, the technical solutions for new service environments such as IoT devices and their interfaces with telecommunication and service networks are not yet in line with international standards. At the same time, services based on technically outdated solutions and services are using new technology. Future information and communication systems must be designed and adapted to work in this challenging business environment where different types of risks, security threats and cyber threats are present.

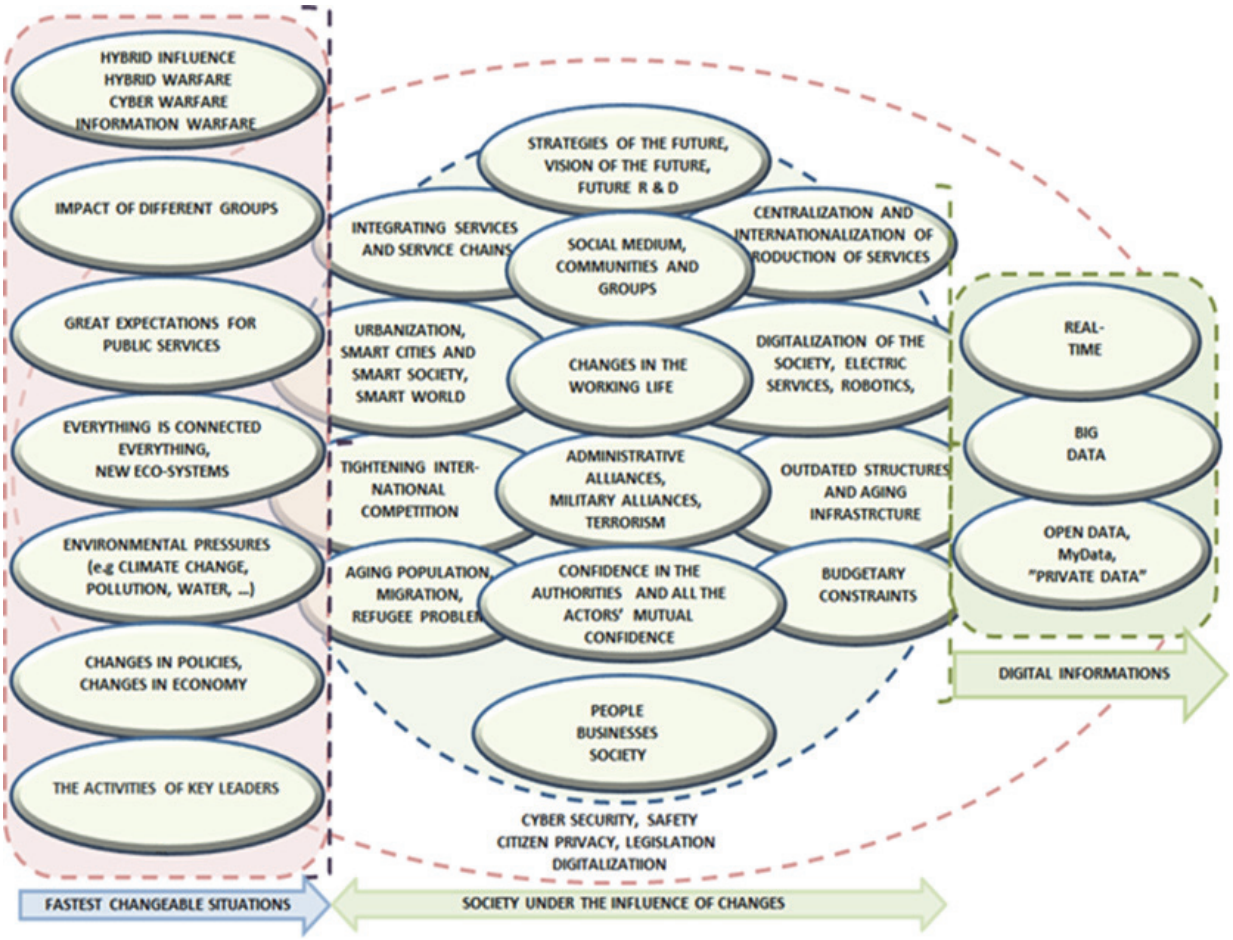


FIGURE 5. Variables affecting the future society.

The research focus of this presentation is limited to examining the key elements of the future society, the smart city. Its activities can be divided into different service sectors as shown in Figure 6. Each set of operations has its own service and communication needs depending on the user group. Such groups include the design and maintenance personnel, financial staff, telecom operators, service operator personnel, virtual service providers and operators, administrative actors, security and rescue authorities and citizens.

Each group of users operates horizontally in their service sector inside the segments (Figures 6 and 8). In order for the smart city to function properly as a whole and to provide citizens with the necessary digital services, the information systems in the various service sectors need to be able to work together and exchange information so that the services of the smart city can be implemented flexibly and efficiently. Information systems used by different service sectors or smaller entities within them are often, however, in different phases of their life cycle. Consequently, the integration between the data models, operating systems, management systems and application interfaces does not succeed for many technical reasons. Their coordination and the success of the data exchange through integration environments takes too long. Additionally, system platform solutions delivered by different vendors often have their own de facto standards that are incompatible with equipment and systems from other equipment vendors. This may result in the use of certain types of platform solutions to

guarantee the functionality of a particular system until renewal is worthwhile or until it becomes timely with the end of the lifecycle. Systems' and services' security solutions may also be different and even partially incomplete leading to practical challenges; for example, it may be impossible to combine the various systems (make federations) and consequently to make different services compatible. Each entity may also contain information at different security levels, which must be properly taken care of, to protect and control them.

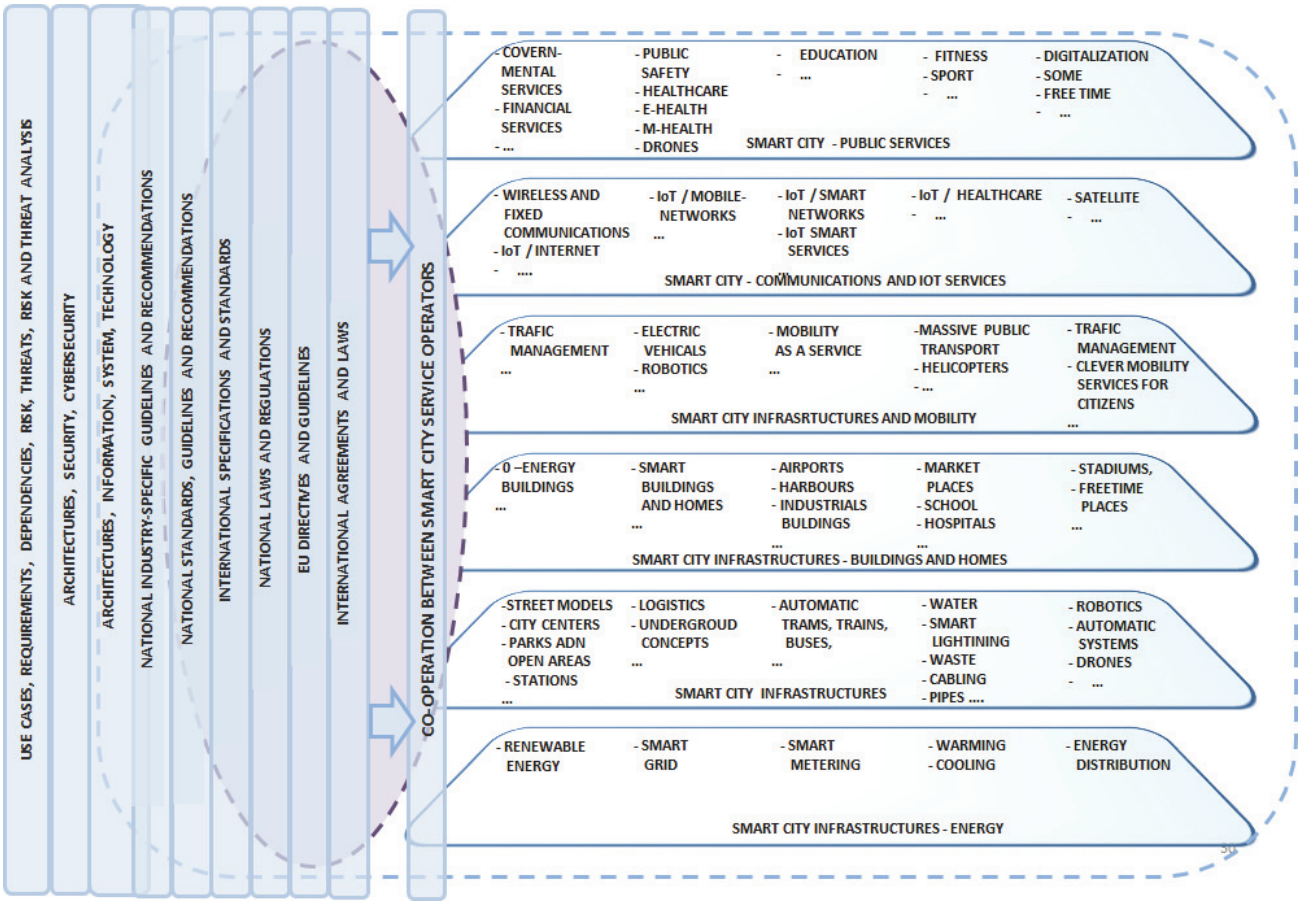


FIGURE 6. Smart city services and infrastructures.

2.2 Objective and grouping of chapter

The purpose of this study is to find a mathematical model to facilitate the evaluation, comparison and analysis of cyber threats. The results obtained through the model will facilitate the design and implementation of architectural solutions. The mathematical model can be used to assess the risk and cyber-threat scenarios of future telecommunication environments and their impact probabilities. The study utilises the smart city's operating environment as introduced in Figure 6, where services and infrastructure are grouped into service sectors. The service sectors are divided into smaller subdivisions allowing risks and cyber threats to different services and systems to be more accurately defined, evaluated and analysed. An examination of threats can be made in the various service segments with regard to the services within them, the

exchange of information between the service segments, the federations required between different operators, the services provided to the inhabitants of the smart cities, the services provided by the service operators and, for example, the economic activities. All future services to smart cities and information societies will be implemented into the telecommunication networks and data centres. The above-described integration accelerates at all levels of functionalities, in each region, both horizontally and vertically. Rapidly growing volumes of information, the latest technologies, newest services, and applications in these intelligent environments make evaluating cyber threats even more difficult. These considerations are taken into account when selecting the target area for the final dependency analysis, cyber assessments, risk assessments and analyses. Section 2.3 sets out the research questions.

Section 2.4 describes the future operating environments and presents the ecosystems and collaborative groups formed by active nodes. This section also presents the architecture model that describes the current and future operating environments of the telecommunication networks and data centres at the general level. The virtual management and control systems of the telecommunication networks and data centres form part of this whole.

Section 2.5 describes the data network and measurements, which were developed to work as platform to the situational picture systems and national rescue information system. They are used in measuring Multiprotocol Label Switching (MPLS) and Dense Wavelength Division Multiplexing (DWDM) networks technologies and functionalities. Section 2.6 presents communications systems with different types of security protection systems. Section 2.7 presents Electromagnetic Pulse (EMP), Electromagnetic Compatibility (EMC) and High Power Microwave weapon (HPM) issues and protections. Section 2.8. describes the cyber-threat levels and the Quality Function Deployment (QFD) models which are used to conduct a threat analysis of the smart city network's infrastructures and services. A threat and risk table for cyber threats and risks is also presented, which provides mathematical modelling for cyber-threat using attack tree-based risk analysis. As the author investigated cyber threats and vulnerabilities, threat-driven analysis and professional knowledge were used to help investigate cyber threats and vulnerabilities. Sensitivity analyses can also be used in the identification of initial threats and basic works. Section 2.8 presents the calculation principles for the probability of risks and threats. Section 2.8.1 presents an analysis for cyber-attack profiles and countermeasures and Section 2.8.2 presents the threat analyses. The mathematical model provides a coherent and comparable picture of the threat, and these advanced definitions can be used to define any additional protection needed and to upgrade the communications networks and data centers architectures. The last chapter describes the conclusions and future work.

2.3 The following research questions are addressed in Chapter 2

RQ 1. Which tools can we develop for the future communications and information architectures in smart cities?

RQ 1.1. Which tools can we use to find dependencies between information systems, communications systems and different services?

RQ 1.2. How can we implement services into a future society and its smart cities in such a way that citizens are able to use them safely in their everyday lives?

RQ 1.3. Which way can we decrease energy consumption in communications and information systems in smart cities and smart societies?

RQ 1.4. What tools can we use for calculating the probabilities of cyber threats to smart cities and smart societies?

2.4 Description of the future operating environment

The future society and smart cities will provide a wide range of services to citizens in real time, regardless of location or time. In this environments, the data streams between the active nodes will be formed. Active nodes include the user terminal devices that exchange data directly between themselves (D2D traffic), the wearables, the HUBs using wireless technology as part of active node communication, IoT devices and M2M devices. In the illustrated concept, almost all devices use wireless technology for mutual communication and for communicating with telecommunication networks and services. Active nodes can form groups and subgroups where the data is classified to different levels of protection: public, restricted, confidential, secret, and in some situations, top secret. This classification has to be taken into account in both wired and wireless networks of homes, office buildings, hospitals and apartment structures and in virtualised networks and data centre solutions and other virtual environments that share information from the user terminal to the entire service chain.

As a technical manager of authority systems and architect at the Finnish Ministry of Finance, the author was involved in developing communications systems and technologies, different types of communications services, the data centers and related services, encryptions systems, organization processes and infrastructures (Figures 7 and 8).

The development of systems and our organizations' processes is often based on an Enterprise Architecture (EA) framework (Dragon1-open) (JHS 179). Figures 4 - 6 and 8 show how complex systems are becoming and how many things need to be considered in our evolving environments if we want to develop effective solutions and clear roadmaps for their development. Figure 7 shows one example of the research, development and strategy work that large organizations, such as smart societies, smart cities, ministries and large companies, should undertake to ensure that strategies, development of environments and systems developments move in the right direction in the future. The EA framework helps us to do perform the development work (Dragon1-open) (JHS 179). That kind of work must be ongoing and must form part of the organization's basic processes (this is my one observation). When this kind of work is continuous, we are able to form a better understanding of the current situations of our systems, whereabouts they are in their life cycle, what parts of the systems need to be transformed into new systems and how best to incorporate new applications.

In the Finnish Ministry of Finance, this kind of work was ongoing and helped the author to research and develop the architect's pictures of the future (Figures 6 and 8).

When our architectures accurately describe the current state, it is easier to identify future needs and develop systems, and to analyse the risks and security and cyber security threats in our environments (QFD INSTITUDE) (University of Cambridge) (Wang, Liu). Those works allows us to better understand the entity as a whole when making analysis and evaluations. One of the most critical issues in the future smart societies environments are exponentially increasing security and cyber security threats, which must be consider in the research and development work, Figure 7.

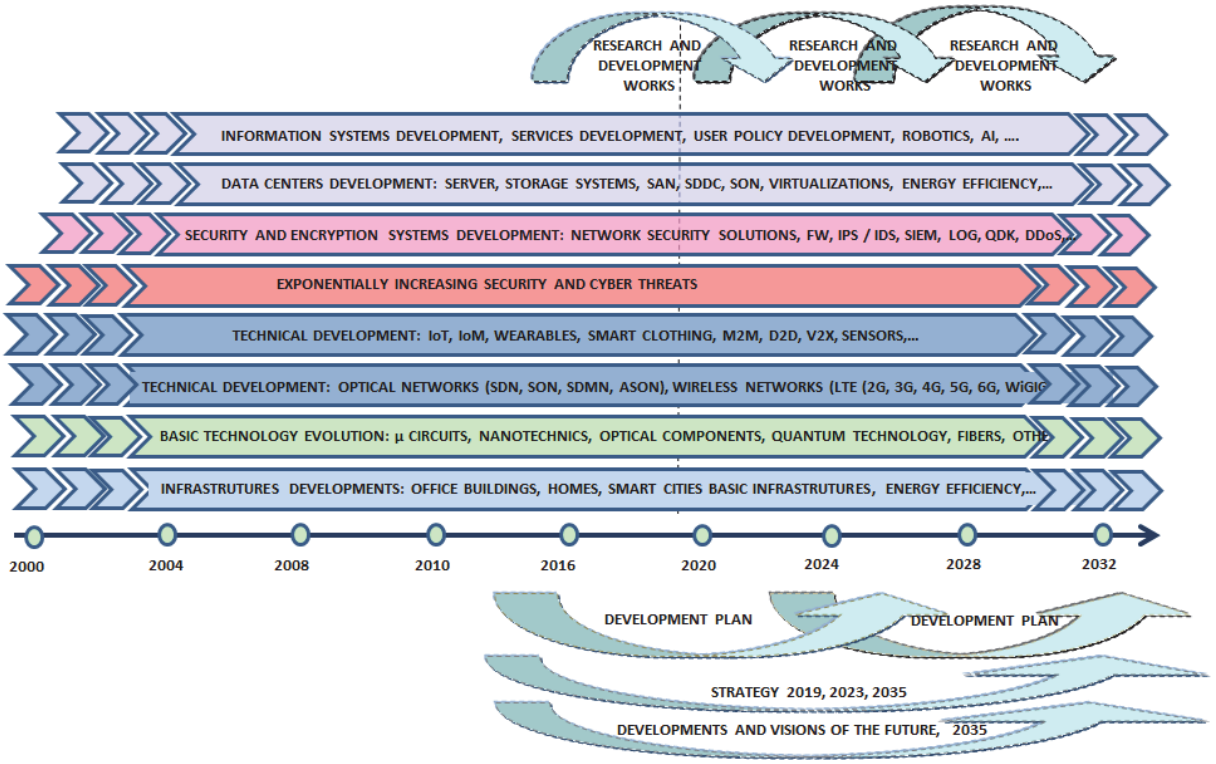


FIGURE 7. An illustration of the research and development work.

Based on the research and development work done by the Ministry of Finance and the work on architecture and security architecture in security authorities environments, the author has created the network architecture models shown in Figures 6 and 8. These figures visualise that in the future, telecommunications systems and services will work in a virtual operating environment where the resources of telecommunication networks and data centres are shared among the users of networks and services by orchestrating different service operators, either together or separately. These virtualised systems will work on wireless or wired networks (see Figure 8). For these environments, the author made virtualisation calculations to demonstrate how much our energy consumption is reduced when we virtualise our data centre systems and communications systems (Appendices 1 and 2). Virtualising our systems also reduces the system costs and CO_2 values (see Table 1 Appendix 1). This virtualisation work is time-consuming because there are hundreds of systems to virtualise. The next step in reducing the power consumption of data centres and communications networks is to use technologies provided by Software Defined Data Centres (SDDC), Network Function Virtualizations (NFV) and Software Defined Networks (SDN) (Figures 8 and 9). However, in the future, implementing virtualisation in this way is unlikely to be sufficient based on the

prognoses which show how rapidly the amounts of information and the energy needs are growing. Therefore, we also need to determine the profiles of the user equipment and the network and data centres equipment based on the amount of time in which devices are really used so we can reduce also our energy consumption in the service chains and services in this way (Appendices 1 and 2, Figure 3). Appendix 1 Tables 1 and 2 show how much virtualisation can reduce the energy consumption. The same tables also show how much CO_2 is reduced when we perform virtualisation. If we have 1000 servers and we need only 100 servers if we use virtualisations, this means more than 2000 tons CO_2 saving per year using virtualized servers. The calculations, based on measured values, showed that the applications consumed only 5% - 8% of the total server power. Therefore, the calculations use a 1/10 virtualisation ratio, taking into account the requirements for rush hours. Rush hours means that there are a lot of users working same time and using same servers systems.

When we consider IoT devices, sensors, actuators and other devices, we can use new type zero-energy communications technology to reduce the energy consumption further because the number of these devices is growing exceptionally fast (Figure 3). The new type of zero energy communication technology means that the device only transmits information when needed and charges its required energy from the radiation energy of its surroundings.

Regarding the entire service chain from data centres to user terminals, virtualisation and implementation of related management structures is challenging because cyber-security in the networks must be managed in the service chains from the beginning to end with their dependencies and risks in mind (Figure 9).

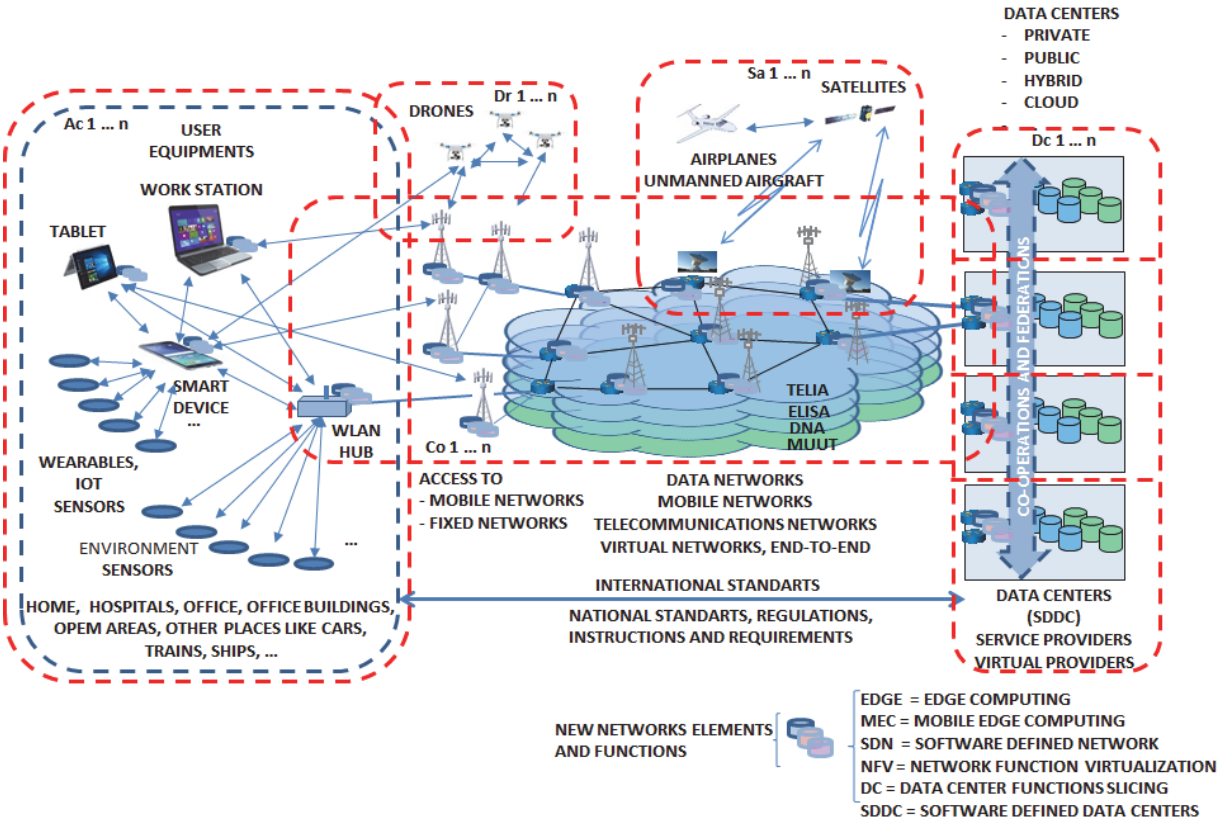


FIGURE 8. Network architecture.

Future environments will require many different security zones, gateways, orchestration and integration in order for services to function in a desired and flexible way. Therefore, it is necessary to manage services users, user access to management services, managements of shared services, infrastructure services and critical services, and management of sliced service groups in virtualized networks (Figures 9 and 10).

Figure 9 shows virtualised communications networks and virtualised data centres, management systems and operators' responsibilities in these environments. In virtualised networks and service environments, all services use the same communications resources, servers resources and storage resources from beginning to the end. In the future, we should be able to communicate within these virtualised environments; in which the data can be classified into different security levels, and there may be multiple layers of encryption depending on the data, and data protection needs of the mobile or fixed networks. However, these virtualised environments will suffer from many cyber security threats because everything is connected to everything else and all smart devices use the same communication environments, as present in Figures 8 - 10. In this environment, these devices will have many deficiencies and dependencies, but dependencies cause risks. When considering the various devices in these operating environments, in Figure 8, we can identify their vulnerabilities, which create risks and threats. These dependencies can also be viewed using the QFD model, and the threats and potential threats analysis can be performed based on attack tree models (PI - PV) (QFD INSTITUDE) (Wang, Liu).

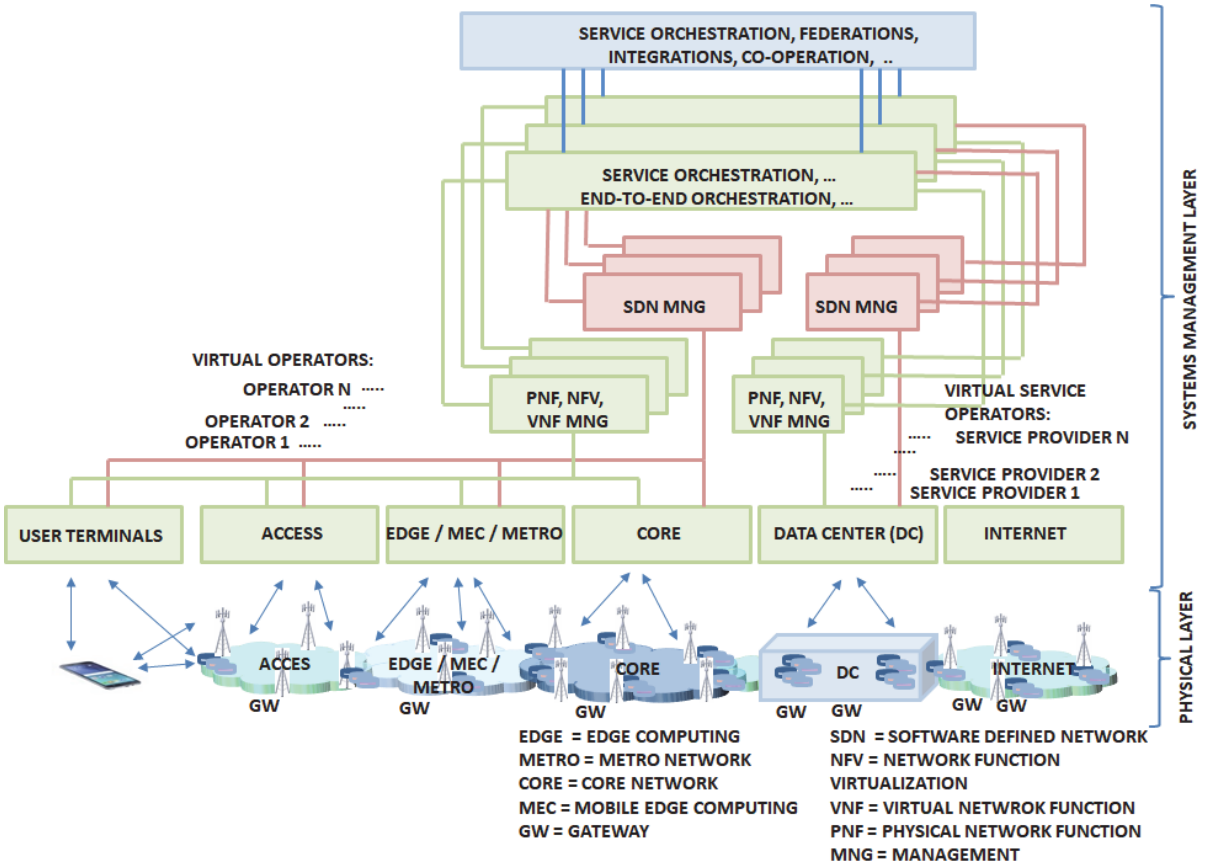


FIGURE 9. The future virtualised communications systems managements.

The vertical and horizontal view of smart city services and infrastructures can be seen on the top level of Figure 6. The different domains like communications and public services, shown in Figures 6 and 8, can be shared to multiple logical networks (or 'network slices'), as shown in Figure 10. The future communication network architecture in Figure 10 includes different slices for the mobile broadband, healthcare, IoT, security authorities, police operations, rescue operations and the physical infrastructure resource.

When regulating and preparing legislations, designers and authorities of networks and services must take into account the changes affecting society (Figures 5 – 6) and the resulting massive amounts of data they generate. Such data types include 'Big Data', 'Open Data', 'MyData' and 'Private Data'. These are further associated with real-time, digitalisation, aging infrastructure, the aging population, global competition (globalisation), urbanisation, environmental pressures, political climate, interest groups, refugee problems and climate change. Registry holders must demonstrate that the preserved data is protected under laws and regulations, and this must be verified, if necessary, in practice ((European Parliament of The Council, 27.5.2016).

One important issue of all the environments, communication networks, data centres and information systems with services is synchronisation; all systems and devices must work together with the same synchronous clock time (Viestintävirasto, 17.12.2014). This synchronisation is required because our Network Operating Centre (NOC) contains all the management and configuration systems and where the Configuration Management Database (CMDB) system and Security Operating Centre (SOC) work together. Network operators use intrusion detection system (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM) and other analysing systems so they must have a clear picture about what is happening, when it was happening or happened, and where it was happening in their networks, systems and devices so that they can start the needed protections operations against attacks. This is one of the most important issues in our communications and information systems environments.

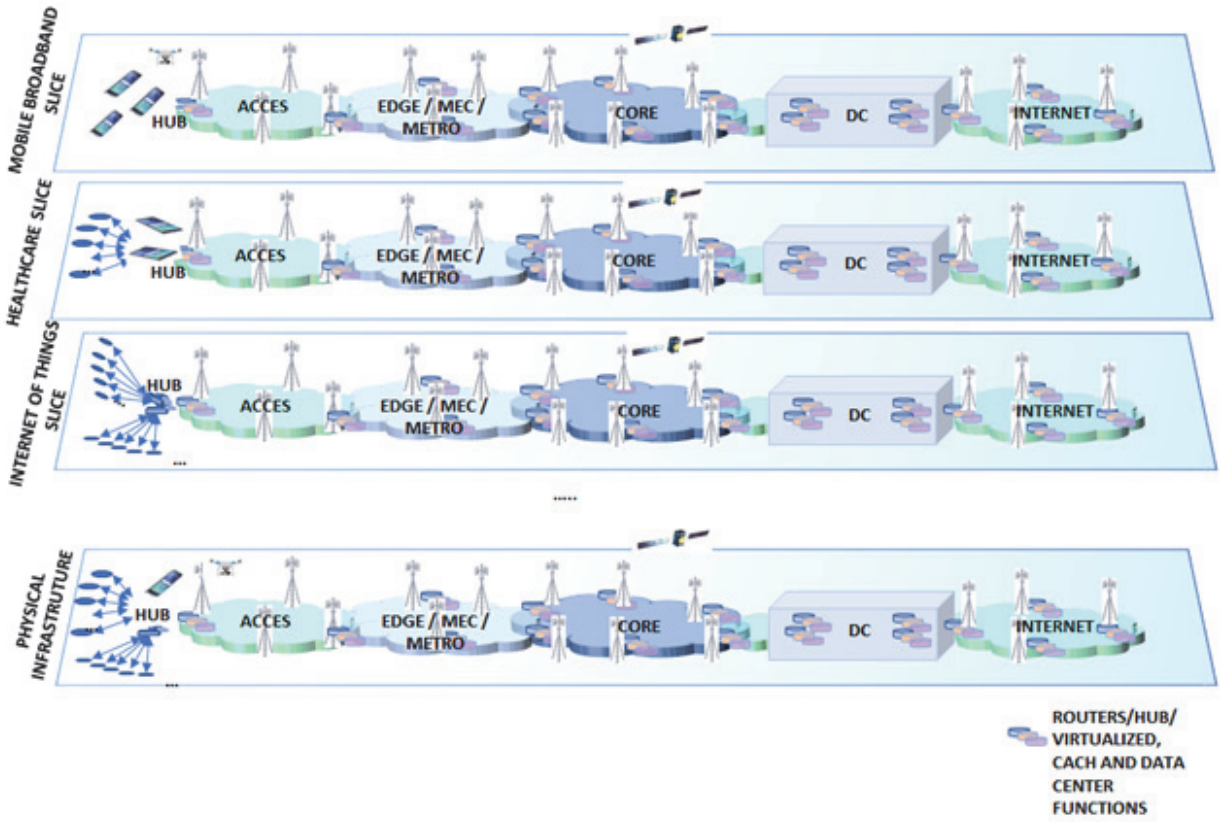


FIGURE 10. The future network architecture with slicing.

2.5 Data network with MPLS and DWDM technology

The MPLS network uses DWDM systems wavelengths (Figures 8 – 10); however, this setup also raises security challenges in networks because different types of devices are connected to MPLS networks via access networks (Figure 11). Additionally, connected devices use the same network resources, and there may be many vulnerabilities in these devices. MPLS network devices are updated after five to seven years because of technical developments and the capacity needs of network resources. By combining different intelligent devices through access networks and backbone networks, the vulnerabilities of these connected devices pose many cyber threats to future systems and services. Interned and inside networks use different types of security zones and layers so that cyber attackers could not so easily attack our systems stored inside data centres. GW systems developed between different security layers were used to protect higher level information from lower level environments and terminals because those in lower levels systems devices include lower level protection systems. Figure 7 presents the development processes used in the environments.

All used systems and services were audited to identify potential vulnerabilities, risks, cyber threats and security threats. The audit process also checked the implementation architectures and deficiencies.

Between 2008 and 2017, when the MPLS networks were developed, some critical issues arose concerning communications connection delays with variations in delay. This MPLS network is used to establish communications connections between the

various sensors and the situational picture system for different authorities´ purposes in national level and also to establish communications connections between national rescue information system operations centers and system data center for people rescue and first aid purposes etc. This MPLS network is also used as a platform for communication between different authorities in their communications systems. For these reasons, quality measurements of the MPLS network have been made to ensure that the MPLS network is suitable for use as a communication solution for these systems. Because this MPLS network used different authorities´ systems, security and cyber security issues must also be analysed. When there are installing security protections systems like firewalls to MPLS network it means also more delays in communications connections. When in user terminals are used IPsecVPN and SSLVPN security systems together to get better protections against hackers and cyber attackers, this means more delays in communication connections. Also, the quality of the connection used is degraded because the packet transit time is longer or the firewall performance may not be sufficient to this purposes. This problem occurred when ´short message´ messages were used in communicate in a congested situation. These delay values and connection quality values must be measured before taking connections into use.

Many critical applications need a delay < 40 mS RTT to work correctly. Measurements of those delay values were performed for different service chains to verify that it was possible to fill the given requirements for MPLS networks and provide critical services. This delay values means that there cannot be too many GW connections, FW or routers and switchers in the service chains. Those delays values are one reason that the data centres need to be located near to the users (Figure 8). The 5G delay requirements are even tighter because the delay requirement is <1 mS there.

Figure 11 is high level MPLS network architecture in which we can see the ACCESS network, METRO (EDGE – MEC) network and CORE network at one end and data centres with a data centre network at the other end. The tests and verification measurements were done in this kind of environment. MEC = Mobile Edge Computing and EDGE = EDGE Computing.

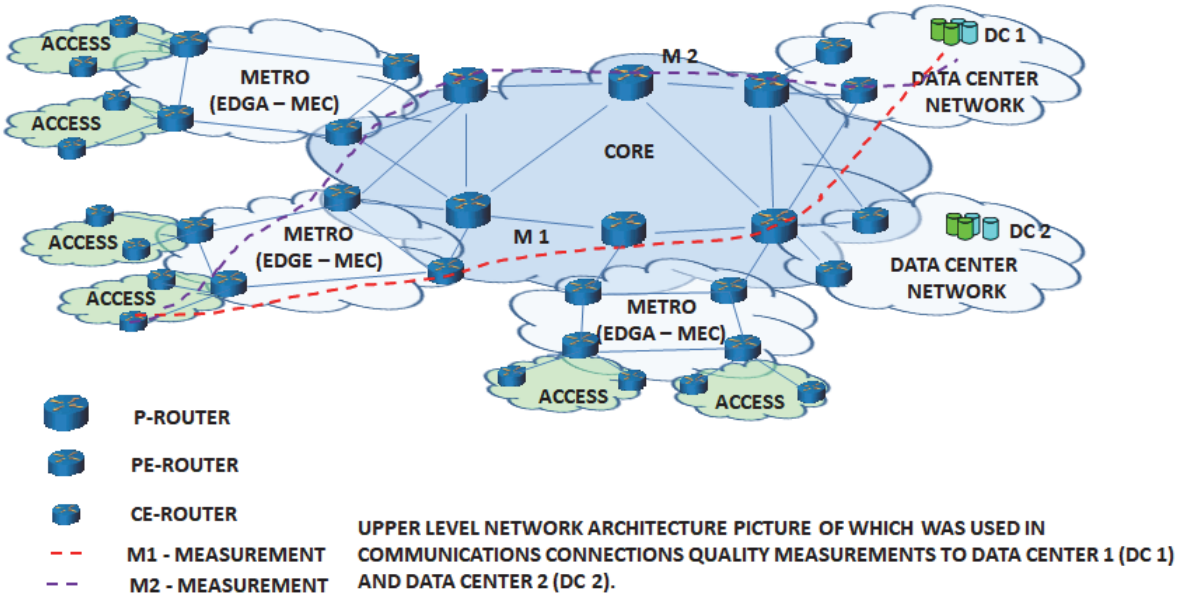


FIGURE 11. Above level MPLS network architecture.

2.5.1 Delay measurements

An example of critical application requirements was a delay value of < 30 mS RTT time. Delay values were calculated in theory for routes M1 and M2, obtaining values of 13.4 mS and 14.4 mS, respectively. When we measured the real values, we obtained 15 mS and 16 mS. These measurements show that this MPLS network meets the delay requirements, indicating that it is also possible to deploy this network for the most critical application environments like rescue applications. Delay measurements were conducted in the same way between other access network nodes and data centre servers (Figure 11).

We also measured the availability of the rescue service and obtained values of a few mS to some seconds. We expect the access times for cellular networks base stations access and terminals to become much larger, indicating the challenges we expect to face with critical communications over cellular networks.

2.5.2 Network capacity measurements and routing analysis

Capacity tests use test equipment to generate and analyse traffic in order to determine the network throughput capacity and any limitations that may exist. The network throughput is tested on 64, 128, 256, 512, 1024, 1280 and 1500-byte packets. The results are analysed at packet per second and bit per second levels. In addition, the delays and their variations during the test cycle are considered.

Before the test, the network shall be allowed to return to steady state and no deviations from the state shall occur during the test. Thereafter, controlled breaks are made to the MPLS network for various communication connections to highlight any deficiencies; the way in which configurations appear in the network management and control systems points out the problems that need to be fixed. The protocols used in the tests included Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) and

Multicast Source Discovery Protocol (MSDP) protocols. Table 1 shows the measured values, which depend on where part of the network office building is located and which kind of access networks and protection systems were used. The measured access times varied from 0.5 mS to 5.5 mS.

TABLE 1. The Performance Values from Measurements of the Longest Communications Path Shown in Figure 11.

	UNICAST					
PACETS	**THROUGHPUT**			**DELAY**		
BYTES	**FPS**	**L3 Mbps)**	**L2 Mbps)**	**Min (ms)**	**Avg (ms)**	**Max (ms)**
64	**1329985**	**489**	**894**	**14.2**	**14.3**	**15.6**
1500	**80259**	**963**	**987**	**14.9**	**15.2**	**16.2**

Even though the measurements taken show quite good performance values and delays, we also need to check the throughput with the FW used in those communications connections before using them to deliver services of the critical systems and where we are using encryption systems such as IPsecVPN.

Figure 12 shows the measurements of the throughput. When we measured the delay values of encryptions of IPsecVPN to layer 2 and 3, we get values ~10 uS for layer 2 encryptions and ~100 uS to 1 mS for layer 3 encryptions.

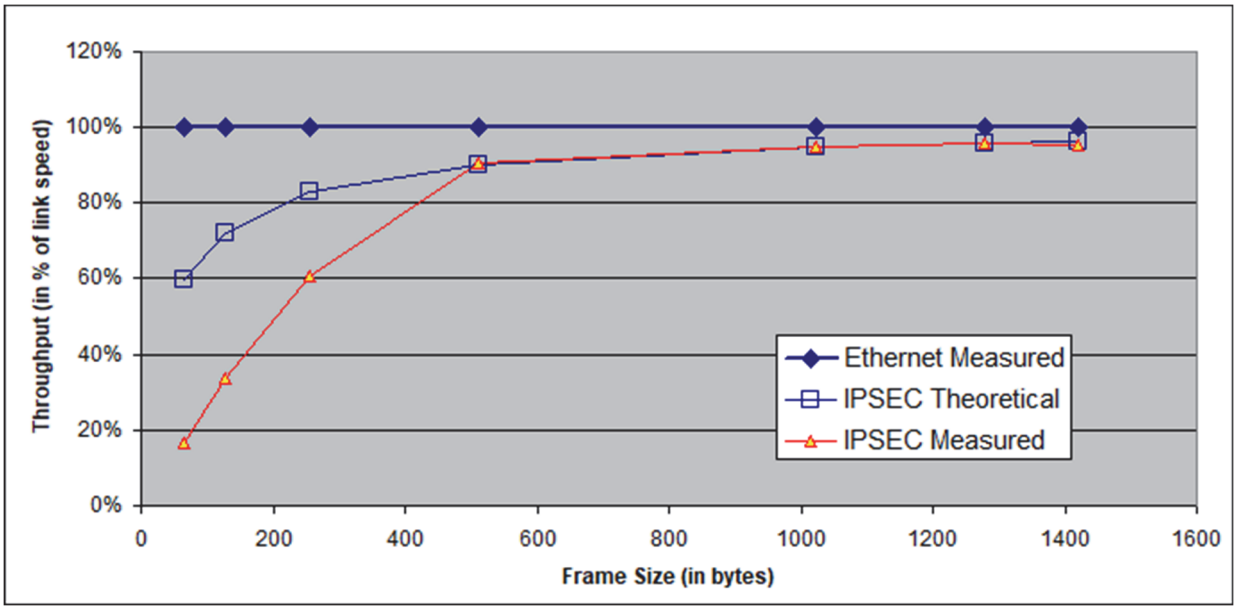


FIGURE 12. The network throughput, theoretical and measured using IPsecVPN.

2.6 Communication systems and protections

Currently, our communications networks typically use DWDM and MPLS technology as a platform for fixed and wireless networking needs. The above measurements show that an MPLS network can also be used as a critical communication and service platform in critical information systems.

Using, sending and working with classified information systems in our networks and environments is becoming more challenging (Figure 13) as networks and service chains require more GW systems, FWs, encryption systems and different types of networks parts' separations systems for network parts (Figure 14). As such, communications environments are becoming increasingly complex and, as many different segments and user groups use the same communications resources, considerable architecture work is needed to obtain a clear picture of these kinds of communications environments (Figures 8 – 10); such work can be performed using the EA framework (Dragon1-open) (JHS 179).

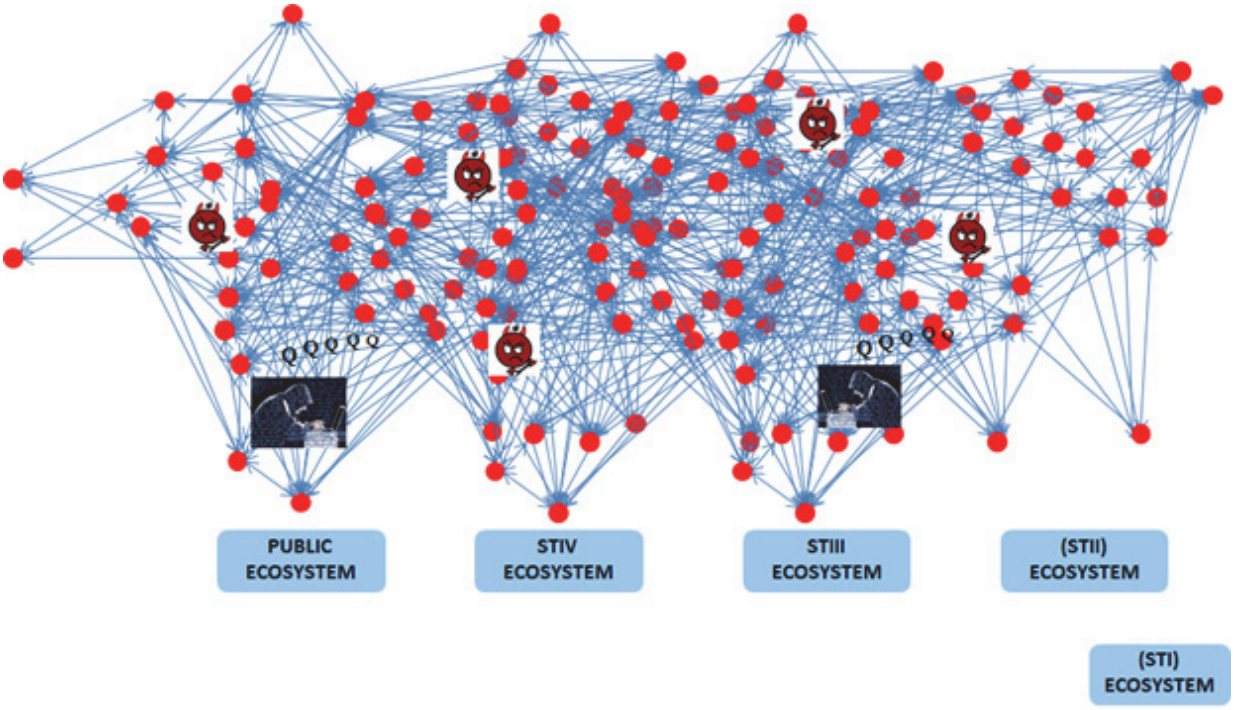


FIGURE 13. Active nodes of ecosystems and information flows in smart societies.

Figure 14 classifies information into different groups to prevent classified information from being transferred to higher or lower level information systems without passing security mechanisms. Figures 8 - 11 do not contain such separation systems. In this dissertation is used next abbreviations of the levels of protection; ST I Top Secret, ST II Secret, ST III Confidential, STIV Restricted and Public terms.

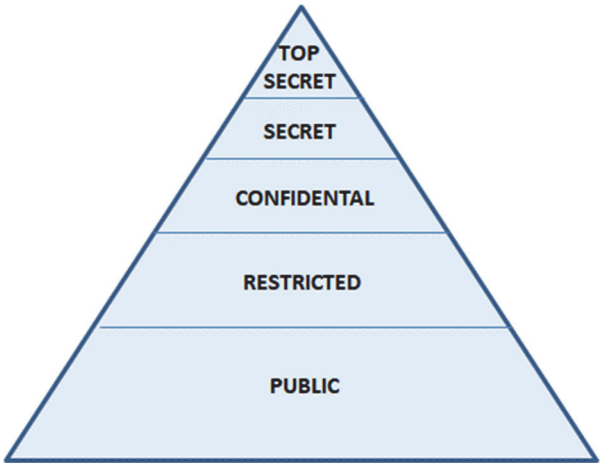


FIGURE 14. Information classification to different classes.

When transmitting data between different classified zones, we need to take care of the regulators' recommendations (Figure 15). This distinction has to be taken care of wherever data is generated and used, such as in hospitals, business centres, office buildings, leisure areas and homes etc. Figure 15 shows that the communication links of the service chains go in one direction only, but as we also need to send communication back to the sender, we need the same type of difference between different classified information when we transmitted information back to sender. Figure 15 presents a GW solution between different classified zones used currently in networks and service entities.

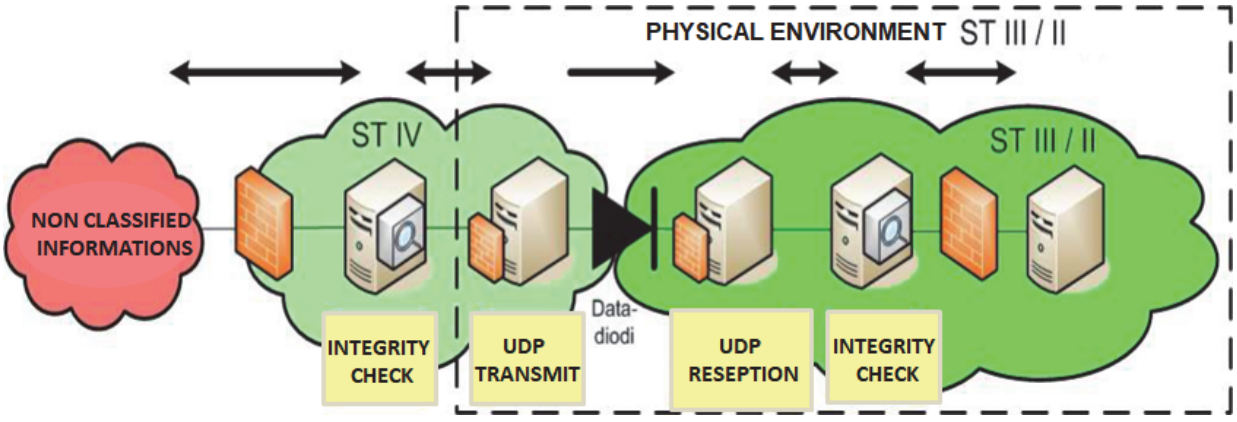


FIGURE 15. A GW solution based on Finland's regulator recommendation of a one-way communication direction.

Previous research has also presented a GW recommendation for virtualised network concepts and connections through a virtualised environment (Traficom, Viestintävirasto, Yhdyskäytäväratkaisu, 20.12.2018). Figures 6, 8 and 10 show the different segments of future smart cities. There are many other communication needs between users and data centres, and between the different types of separate segments.

Such segregation of classified information is required on both the access terminal and data centre sides and in the network connecting the systems. When we are developing our communication systems and services, we must take into account the national recommendations and the European Union's recommendations concerning security, privacy and cyber security issues.

2.7 EMP-, EMC- and HPM protections

In 1983, the Finnish government and security authorities made the decision to start building Electromagnetic Pulse (EMP) protections in Finland, and in 1984, the designing and building of EMP shielded rooms commenced on the security authorities' side. The requirement was to build EMP shields with sufficient attenuation to resist EMP explosions, which could occur in a high altitude atmosphere. These requirements came from component destruction values that were verified by measurements to determine failure probabilities. At that time, the author was developing physically protected rooms with sufficiently high attenuation requirements in accordance with the given requirements for measurements systems. The same group also developed an EMP shield attenuation measurement systems which could be used everywhere measuring shield attenuations values. As part of a group, the author also developed an EMP protection guide for Finland, and from 1989 to 1993, he worked in the international working group IEC/ WG 77 to develop the EMP and EMC standards (LM, EMP-suojausohje, 21.6.1989).

The introduction of High Power Microwave (HPM) weapons in the 1990s presented more challenges to the EMP protections systems, meaning that the protective systems had to be modified, measurements had to be made at higher frequencies and any weapons that had a potential direct impact on the target, needed attenuation values had to be checked in all critical environments. These days, HPM attacks are typically conducted by drones which carry so-called small bag HPM weapons that are easy to carry near the target (Hämäläinen, Järviö, Kuja-Hakola, Silvola, Paunonen, 2009).

Inside the shielded rooms which include all the installed devices people use such as network devices, data centre devices and smart devices, we must ensure EMC protection. Radio frequencies are the easiest way for hackers and cyber attackers to collect information from organisations or individuals and to attack services (Azade Fotouh, Ming Ding, Mahbub Hassan, 26.10.2017) (Takahashi, 1.18.2016).

Hackers and cyber attackers usually take advantage of vulnerabilities in the communications connections of our networks and service systems. Attackers also connect directly to cables inside buildings, through manholes in the streets or at connection points at the sides of highways to collect critical information or attack their target organisations. Drones have also become effective devices used for spying on and attacking fake base stations (Figure 8), enabling attackers to collect information that they use to gain access to our networks and services and to attack our systems. EMP, EMC and HPM shielding can be installed and used to protect our systems everywhere needed.

The author was involved in developing EMP, EMC and HPM shielding and protection systems for many years.

2.8 Cyber Threats and the QFD Model

For work in all cyber threat and attack situations, it is essential to determine the dependencies and risks for security and cyber threats by carrying out risk analyses across service and supply chains. These network areas, network sub-areas and network operators´ responsibilities must be considered in a virtualized environment (Figures 8 and 11). This evaluation provides a better understanding of the whole entity when conducting analyses and making evaluations.

To assess the threat level, estimates of the cyber-threat levels, the attacker abilities, motivations and target areas are made (Table 2) (Finland´s Cyber Security Strategy, 2013). Then, the QFD model is used to understand the working environment and examine how the entities are formed. The QFD model can be used to demonstrate the interdependencies between different things and systems and thus determine which systems and services depend on each other and what are their effects on each other. At the same time, threat, dependency and risk analyses can be further elaborated with more detailed descriptions (Figure 16).

The increase in services that will accessible via wireless networks in the future will enable people to use the services offered to them while travelling from one place to another, for example, by car, train, tram or ship. As a result, attackers will have an increasing number of opportunities to penetrate systems and services by exploiting vulnerabilities in terminal devices or by accessing the network; it is not always possible to deliver services in a managed and controlled network environment where the security is in order. When an attacker hacks into the system, they can execute the desired operations without being noticed and thus before the proper response can be made to initiate countermeasures. In the layers of different QFD models must also take into account the levels of data protection. The protection levels must be taken into account in the physical structures and in the telecommunications and information technology systems.

In Figure 16, the first layer consists of the access networks (wired and wireless) of the telecommunications networks, followed by the layer for the EDGE – METRO network and the regional and backbone networks. The third layer consists of systems that make up the necessary GW systems between the telecommunications networks and the data centre. Inside the data centres, the next layer contains the servers, storage systems and middleware systems. The next layer includes application servers and applications. The services offered by the data centre are put in their own layer because the use cases and requirements define their operating environment with their systems, where the services rotate and where the services are offered outward. The last layers in the model compare existing information systems and present the needs related to their interactions. For each layer, the required operating environment and services provided by the information system and service can be defined. From that information, we can define dependencies and analyse the risks and threats. Every service or communications need starting point is to make scenarios and view use cases derived from scenarios.

From scenarios we get requirements and from the requirements we can define services and from which we can lead the requirements of the projects, requirements to operating environments and to systems, and to define system requirements and functional and technical requirements for them. One criterion to define requirements is

the criticality of the service. All requirements can be presented in a table format, which makes it easier to apply the requirements for each service and system, and to compare the requirements (Helferich, Herzwurm, Schocker). From the calculation table, it is then easy to determine the lifecycle costs for a service, system or device, taking into account its energy efficiency and ecology (QFD INSTITUDE) (University of Cambridge) (European Parliament and of The Council, Energy Efficiency, 25.10.2012) (ENISA, 2017), (Appendices 1 and 2). All this activity is guided by user organisations with defined cyber, technology, information and security policy, telecommunications policy, strategies and legislation. User organisations use also international guidelines and directives and international standards. The QFD tables make it easy to see where service is used for each information system, and what service and software upgrades should be made when updating the information systems (QFD INSTITUDE) (University of Cambridge). This is happening inside the service chains and also those in a virtualized environment in the entire service chain (ENISA, 2017). Since the data used by the model and the values derived from the sensitivity analysis can be mapped, mathematical analyses can be used to analyse the information presented in the tables.

TABLE 2. Cyber Threats

Cyber threat levels	Attacker's capabilities	Attacker's motives	Attacker's target
Cyber warfare (Strategic) (Tactical)	Very sophisticated attackers; capable of multiple, coordinated, continuous attacks	Political or military dominance	Society, politics and military critical infrastructures
Cyber terrorism	Sophisticated attackers, capable of multiple, coordinated attacks, are able to establish a persistent foothold within the organisation's infrastructure	Bring uncertainty to society and its functions, political or military environments	Society, politics and military infrastructures
Cyber espionage	Attackers with moderate expertise capable of launching multiple attacks, seek to gain a foothold in the organisation's infrastructure	To get of property and services	Governments, companies, individuals
Cyber crime	Attackers with limited technical expertise; aim to acquire critical information to use	Economic gain	Companies, individuals, governments
Cyber vandalism, hactivism, hacking, …	Attacker's personal knowledge is not so high; non-targeted attacks, primarily focused on obtaining an organisation's data	Political change, personal enemy, EGO.	Governments, companies, individuals, other

The QFD model, shown in Figure 16, consists of ten functionally separable layers. In different cases, the threats can be looked at in terms of operating environments, systems functionality, and action queries to seek potential shortcomings, weaknesses, or vulnerabilities in their security mechanisms (Fitch, Muckin, 2015). Cases can be grouped into so-called fixed and mobile network environments on the one hand and/or virtual network environments on the other. Reviewing cyber threats can be done in a process-like manner by estimating how the hacking would proceed and with which mechanisms the attacker(s) would proceed toward their goal. Mechanisms may vary depending on the attacker's ability and technical capabilities. The following is an example of a mechanism used by attackers (Heinzmann, Steffen, 2012) (ENISA, Threat Taxonomy, January 2016): Footprinting (to collect information of the target), Flickprinting (identify the topologies and systems), Sniffing (collect network traffic), Enumeration (collect access information), Scanning (detect systems and services), Gain Access (use passwords, vulnerabilities), Escalate Privileges (pilfering, vulnerabilities), Create Backups and backdoors (install programs), Cover Tracks (clear logs, hide tools) and perform Distributed Denial of Service (DDoS) attacks.

The analysis can be deepened and widened using documented descriptions of software vulnerabilities as an aid (MITRE, 2017). The following can be used to deepen the review: Injection, Improper Authentication, Management of Credentials, Permission and Privileges Management, Cryptographic Issues, Data Management, Improper Input Validation, Insufficient Verification of Data Authenticity, Improper Certificate Validation, Values, Resource Management Errors, Cross-Side Scripting, Race Conditions, Environment and Configuration. In addition, the following entities can be further examined: Confidentiality, Integrity, Availability, Authorisation and Traceability.

For examination, the threats can be divided into internal and external threats. Threats can be caused by individuals, the technical systems or the environment. In these cases, we can also talk about the risks, threats and cyber threats. Sensitivity analysis can also be used to define the threat level. Table 3 presents an example of the threats and risks.

TABLE 3. A Threats and Risks Table

REF ID	ORG	FUNC-TIONS	CATEGORY	THREAT / METHO-TOLOGY	THREAT / RISK	EXIXTING CONTROL	THREAT/ RISK LEVEL			ACCEPT / REDUCE	RECOM-MENDED CONTROLS	RESIDUAL THREAT/ RISK			CHECK POINT
							L	C	R			L	C	R	
1-AM	MC	IDENTIFY	ACCESS MANAGE-MENT	FOOD-PRINTING ...	- INFOR-MATION GATHERING - TARGET ADDRESS RANGE - NAME-SPACE ACQUI-SITION - NETWORK TOPOLOGY. ...	-INVENTORY OF PHYSICAL ASSETS IS MADE, PROTECTIVE SYSTEMS LIKE FIRE-WALLS, IDS, IPS ARE PLACE, VPN AND SECURITY ARE INSTALLED ...	3	3	8	REDUCE	DEPENDS ON SECURITY LEVELS OF ACCESS NETWOKRS AND ITS SERVICES: -PUBLIC -RESTRECTED -CONFIDENTAL - SECRET -TOP SECRET ... EU DIRECTIVES NATIONAL RECOMMEN-TATIONS,...	2	2	3	XX

L= Likelihood, C = Consequence, R = Risk

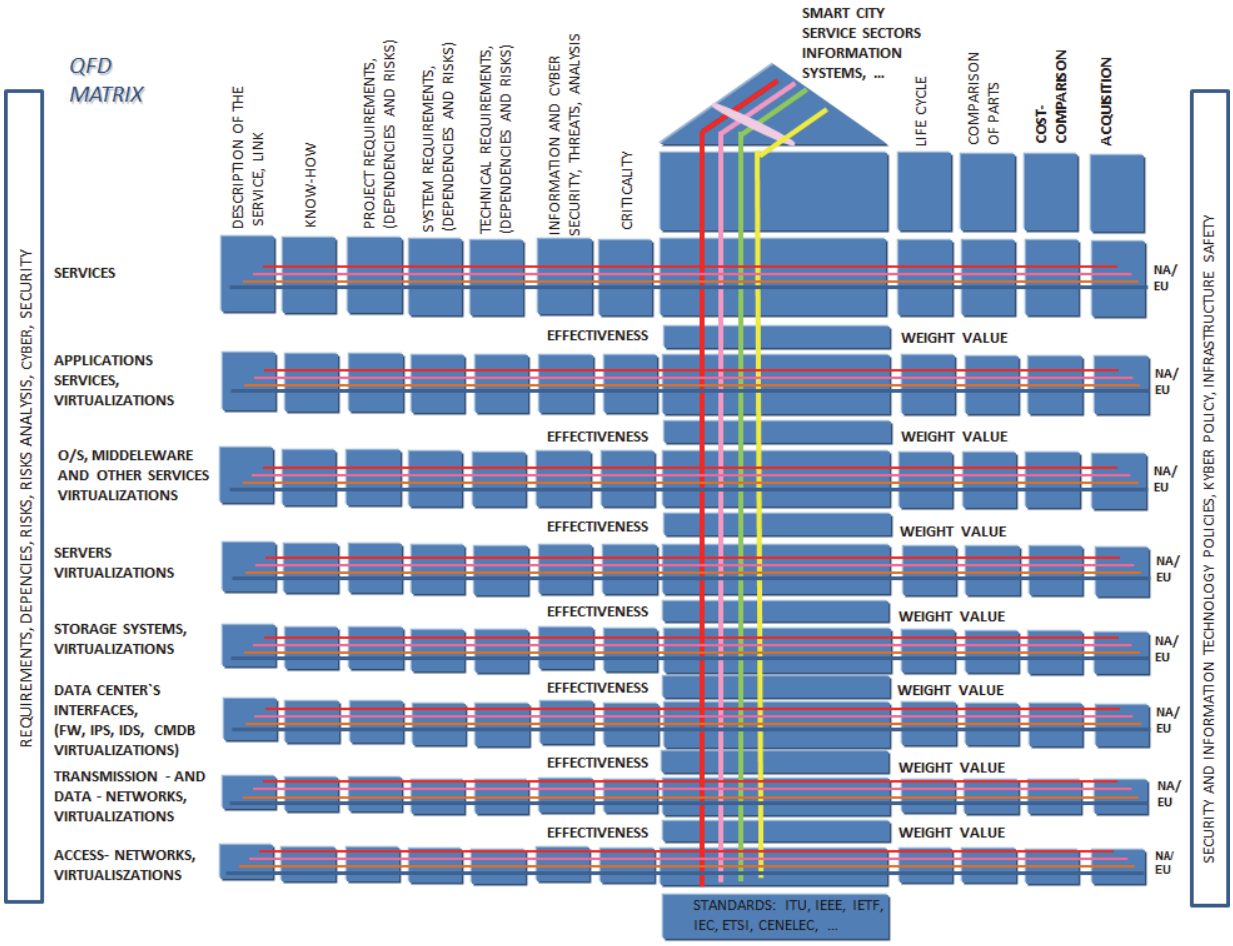


FIGURE 16. QFD model for ICT infrastructures (QFD INSTITUDE).

The operating environments described in Figure 16 must also be considered in a variety of disturbance situations, under exceptional circumstances and in the so-called extreme emergency conditions so that the overall threat situation can be identified and so that the necessary decisions, laws, instructions and architectures can be prepared and updated. When the results obtained using the QFD template are exported to their tables, they can also be used to build attack tree models for various services, systems and service chains as small parts or as a whole.

Figure 17 presented an example of a case where we examined a wearable device and its service chain from the user through its communications connections to the data centre. This type model is used to calculate the risks and cyber-threat estimates also in the next section.

The purpose is to analyse the interfaces of a single entity to identify its weak points, which can then be improved to reduce the likelihood of cyber threats and lower the risks involved. At the same time, we gain knowledge to identify which components have vulnerabilities and thereby improve the end-results in the entire service chain. The model helps to make the threats more comparable with each other to better illustrate the overall picture of the vulnerabilities.

Prior to assessing the threat levels and performing the analyses, we need to conduct risk mapping of the organisations and operating environments of the system entities and smart devices we use daily. The risks and residual risks that are identified,

assessed and analysed will be presented to the management of the organisation and checked in the audit process.

The next is an example of risk survey that the author used in his work and related to his previous work. This risk mapping was done for all levels of the organisation and included the management processes of participating and affiliated organisations such as the design methods, material and software procurement processes, material delivery processes, material acceptance procedures, new systems testing and deployment processes, maintenance processes and the organisation's service development processes.

As can be seen in Figures 7 and 16, a delay in the R&D and deployment of a system and its software in a critical environment can lead to a delay in software updates, which can in turn lead to technical problems and vulnerabilities that can have a critical impact on the system performance and functionalities. Hackers and cyber-attackers typically seek out systems with technically outdated solutions and vulnerabilities so they can easily hack into the systems to exploit the systems and services.

An unmanaged critical risk, or just a shortage in system or device protection, can become a threat that outsiders can exploit in one way or another. About threats in our systems and used devices, detected or hidden threats, we get information from Finland, from Traficom's online resource sources, or through its international cooperation organizations or country-specific research institutes.

Online application stores present a big risk factor for companies and authorities because individuals can purchase different applications for their terminals which may have not been tested and revised by a responsible security unit. Those applications may already contain vulnerabilities or malware pieces that allow attackers to launch targeted attacks against organisations.

Similarly, dependencies, risks and threats across telecommunications networks, information systems and software used therein, and data centres and services need to be addressed to provide overall risk and threat assessments and prepare follow-up actions and responsibilities.

For the purposes of risk and threat analysis, the technical systems and solutions can be subdivided into telecommunication networks and related services, applications and application services, communication services, workstation and communications services, internet services, wireless networks and related services, communications' platforms, servers' platforms, critical information systems, user and access control (IAM). This way it is much easier to search risks and threats and make threats calculations and make analysis to them.

2.9 Risks and threats probability calculations

There are in the world developed various risk and threat analyses methods to detect intruders' attacks, identify systems vulnerabilities, and develop, build and deploy security systems to protect information environments from cyber-attacks. Attack tree (AT) techniques [6] have an important role in investigating cyber-attacks for risk assessment. This study uses protection trees and defence trees to analyse the weaknesses that make the system vulnerable to network threats.

It is difficult to identify the attack profile of possible hackers or cyber attackers over the internet or via other parts of communications networks. Tree structures have been widely used for exploring the potential attack profile by analysing all possible attack paths identified in threats and risks tables.

When we have defined the dependencies, we can put those issues into tables to identify the probability values of the associated risks. Those probability values are made based on a sensitivity analysis with different professional people in ministries in that ICT area. Figures 6 and 8 show that many tables need to be created to account for even the smallest risks in our infrastructure, systems and services, which is time-consuming. Figure 7 presents an example of the research and development work in different systems in the future environments. Every phase of those works involved a risks and threats analysis based on the dependencies and vulnerabilities of systems.

Our development and research works involved assessing about 1,000 information systems and hundreds of applications and more than 30,000 users with different types of terminals. Figures 8 and 11 also show that the amount of required work is impossible for one organisation to perform alone. Thus, cooperation is needed between different organisations.

Because there are in communications and information systems and services a lot of risks, vulnerabilities and threats, the author performed a risk and threat analysis only for access networks environment (PI) and access networks in a hospital environment in the patient's room (PIV). Figure 17 is an example of an access network. This same analysing method can be used to make more calculations to future environments and their communications services and systems and devices.

In these analysis and probability calculations, the author evaluates the competition between the attack and defence actions to determine the possibilities of attackers getting into systems and services. Therefore, the author needs to obtain a clear picture of dependencies and vulnerabilities of the systems and devices, the communications systems, the architectures, the used systems and concepts weaknesses, the protection systems, and people's working methods and processes. The risks of every system and application should be defined, and based on those definitions (in the tables), the risks and threats values can be calculated.

Attack tree technology provides estimations of the probabilities that an attacker will attack the systems in our environments; however, it is just a probability and there are residual risks and residual threats that need to be examined more closely to reduce their ability to influence our systems. We also review these residual risks and threats in our audit procedures and make recommendations to reduce them so that we have smaller risks and threats remaining (Puolustusministeriö, Katakri 2015).

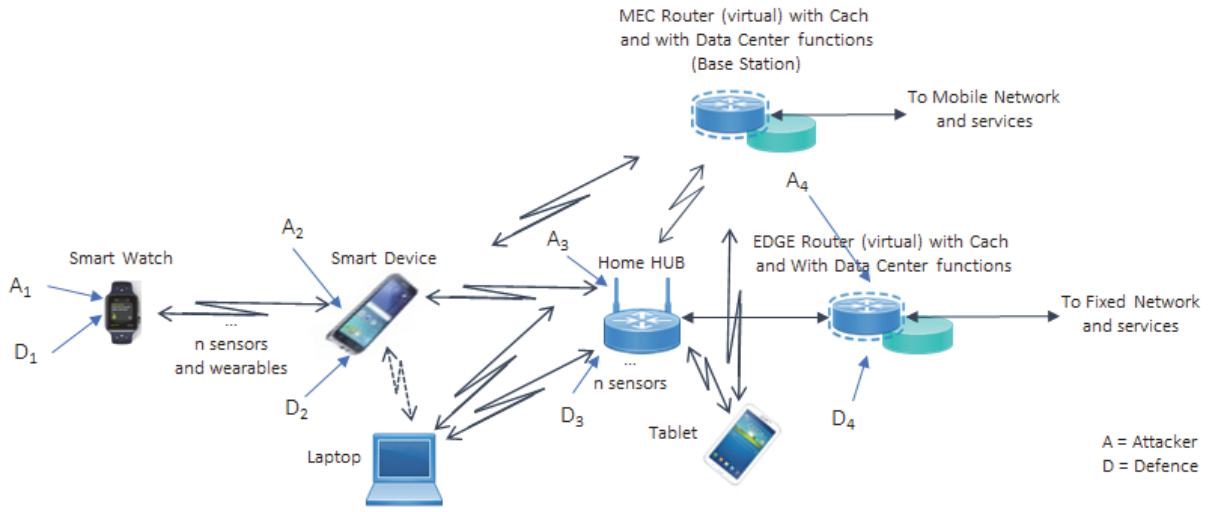


FIGURE 17. An access network with user terminals (one user).

As can be seen Figure 17, the access network environments contain a lot of wireless technology which is likely to increase in the future with the introduction of 5G mobile base stations to many places such as hospitals. values are too high in zero-energy buildings, so that cell phones cannot be used or function properly inside buildings and communicate out and vice versa without a small cellular network at the station. This is already the case in some places (Sayed Fahad Yunas, 9th October 2015).

Various threat analysis schemes such as Attack Trees (AT), Defence Trees (DT), Protection trees (PT) and Attack Response Trees (ART) can be used to identify the risk level and threats of an information asset via accumulating the system vulnerabilities, the corresponding impacts and estimating the attack costs and defence costs.

2.9.1 Analysis model for attack profiles and countermeasures

The first author modelled an attack tree based on the information in the reference model (Wang, Liu, 2014). The model is adapted based on the example system shown in Figure 17. The basic idea is to describe the attack profile, estimate the probability of attacks for each node used and determine an appropriate solution for attack countermeasures.

There are two types of events to consider: an attack node and a defence node. Because this model is too simple to use to model complex attack scenarios and the newest attack methods, the attack events are broken into two sub-events: detections and attacks. The defence event is separated into deception and countermeasures, as shown in Figure 18.

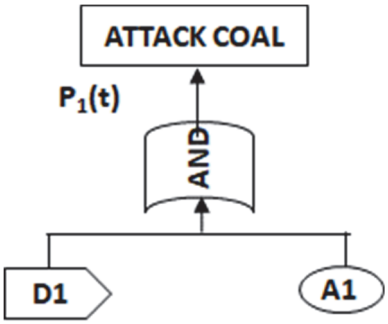


FIGURE 18. An attack tree model.

TABLE 4. Notations Used

ACTION	EXAMPLES	NOTATION
ATTACK	REGISTRY MODIFICATION, OPEN PORTS, …	A
DETECTION	DNS QUERY, PORT SCAN, …	D
DECEPTION	HONEYPOT DEPLOYMENT, …	DE
COUNTERMEASURE	VULNERABILITY FIX, SAFEQUARDS PUT IN PLACE, …	M

As attackers can use distributed attack methods, attacks can come in many different ways and from many directions. An attack tree model thus consists of a detection event and an attack event, many detections events and attack events, and a deception event and many attacks and countermeasures. For probabilistic analysis and calculations, the defender needs to estimate the probability of a successful attack for each node in an attack tree.

The probability of attack success at the coal, shown in Figures 18 and 19, derives from the following five formulas.

$$P_1(t) = p_{A1}(t)(1 - p_{D1}(t)) , \quad \text{(Figure 18)} \quad (1)$$

$$P_1(t) = p_{A1}(t)[1 - p_{D1}(t))(1 - p_{M1}(t)], \quad \text{(Figure 19)} \quad (2)$$

$$P_2(t) = p_{A2}(t)(1 - p_{M1}(t)), \quad \text{(Figure 19)} \quad (3)$$

$$P(t) = [p_{A1}(t)(1 - p_{D1}(t)) + p_{A2}(t)(1 - p_{M1}(t))], \quad \text{(Figure19)} \quad (4)$$

$$P(t) = [p_{A1}(t)(1 - p_{D1}(t)) + p_{A2}(t)(1 - p_{M1}(t))]p_{A3}(t)(1 - p_{M2}(t)). \quad \text{(Figure 19)} \quad (5)$$

The formulas for probability calculations depend on where the detection and deception systems are located, IPS and IDS systems are located, other analytics systems are located, and where we take countermeasures etc. Consideration should also be given to 'hardened' systems and equipment in environments where we use classified

materials and a classified infrastructure. When we calculate the probabilities of attacks to real access networks with all possible systems and devices, the calculations become very heavy and thus calculation programs would be more efficient for performing the calculations. The calculations become even more challenging when considering classified environments, communication networks, and classified services. EA, Reference Architecture, Integration Architecture and Target Architecture are becoming increasingly important in obtaining a deeper analysis of these risks and threats.

Target Architecture is also important because hackers and cyber-attackers use different types of analytics tools to gain information about our networks, systems, and services, so we need to know exactly what information we have. Figures 4 - 6 and 8 show that the increasing complexity of future communications systems, especially when using classified information in classified environments; thus, accurate knowledge is extremely valuable so that we can better protect our systems against hackers and cyber attackers.

Machine learning can be used to perform the calculations more quickly and accurately than when done manually One example of author earlier analysis involved going through more than 6,500 different technical and non-technical requirements to define the risks and threats.

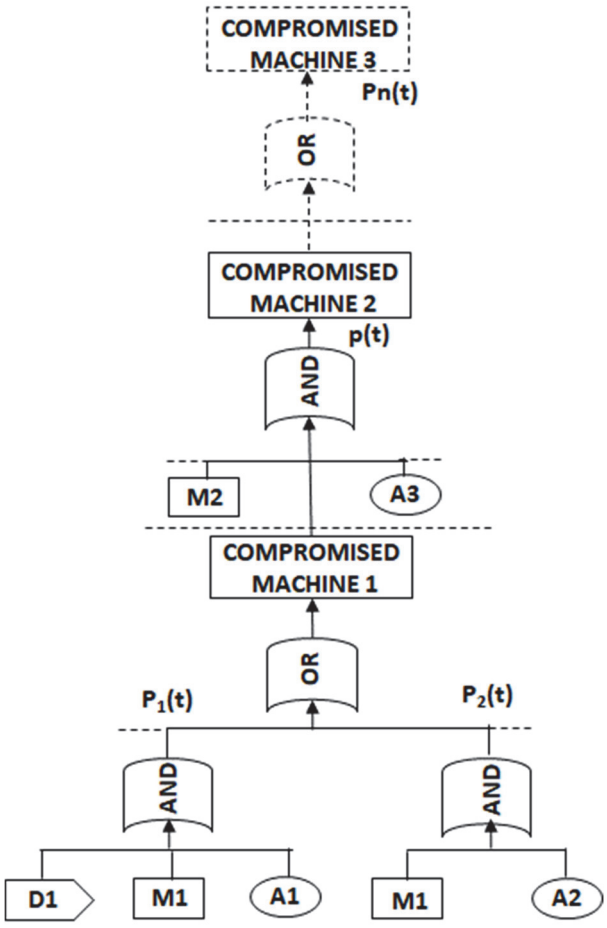


FIGURE 19. An attack tree model in a real network (Wang, P. Liu, J.C., 2014).

2.9.2 Making and modelling of threat analyses

Because it is difficult to conduct a risk and threat analysis for the whole of future society or just an entity comprising the service sectors of the future intelligent city, we divide the whole environment into smaller sections, the service sectors (Figure 6). The telecommunications arrangements required by the service sectors for their services are grouped into segments as shown in Figure 8. The entire network consists of access networks (Ac 1 .. n), core networks (Co 1 ... n), drone networks (Dr 1 ... n), satellite networks (Sa1 ... n) and data centre networks (Dc 1 ... n). The threat analysis is conducted for the access network as shown Figure 17; Table 4 shows the notations. Reason is that access networks are currently subject to major changes and because these involves large quantities of different sensors and IoT devices. The starting point for the analysis is a smartphone interface for the connected wearables, and the connection of the smartphone to the home HUB system and to the EDGE router. The EDGE router is virtualised and includes some services in their own slices in the future. In addition, the HUB system may include FW functions.

The EDGE router and the HUB system may also include features of data centre functions such as switches, storage resources and cache structures. Section 2.8 presented an example of an attack mechanism, showing how aggressive attacks will be done and in which way attackers use vulnerabilities to analyse systems and compromise a target device. These calculations obtain the values for these vulnerabilities. The events must be independent and if they are not, we must go to small entities to reach an independent situation with respect to the various functions. The analysis can be deepened by examining the vulnerabilities of different OSI layers and by analysing the vulnerabilities of the protocols on the different OSI layers. For a probabilistic analysis, the defender needs to estimate the probability of a successful attack for each node shown in Figure 19, in Attack-Defence Tree (ADT). For the purposes of the review, we define the used notations, Table 4, [6]. For deeper and larger cyber-attack estimations, we can use the ATT&CK matrix from MITRE for Enterprise (MITRE, 2019).

The MITRE matrix is divided to several different parts: Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration and Impact.

The calculations are based on the author's earlier works and incorporate only public materials.

TABLE 5. Meaning of Notations used in this calculations example

ACTION	EXAMPLES	NOTATION
ATTACK	SNIFFING, ENUMERATION, SCANNING, …,	A
DETECTION	PORT SCAN, INFORMATION SCAN, …,	D
COUNTERMEASURE	ANALYSING OF VULNERABILITIES AND TO REPAIRING, SAFEGUARDS PUT IN PLACE, …,	M

The probability of a successful attack (P(t)),

$P1_{1\ldots n}$ (t) = $p1_{A1..n}$(t)(1 – $p_{D1\ldots n}$ (t)), (1)
to n wearables

$P2_1$(t) = P1_1(t)[(p2_{A2}(t)(1 – p2_{D2}(t)], (2)
first wearables connection to smart phone

$P2_{1\ldots n}$(t) = [($p2_1$(t)) + (p2_2(t)) + … + ($p2_n$(t))], (3)
because different wearables connect to smart phones at different times,

$P3$(t)= p_{3A}(t)(1 – p_{3D}(t(1 -p_{3M}(t), (4)
laptop

$P2_{13}$(t) = $P2_{1\ldots n}$(t) + [(p_{3A}(t))(1 – p_{3D}(t))(1 – p_{3M}(t)]), (5)
smart phones and laptops connect to HUB

$P4_1$(t)= p_{4A}(t)(1 – p_{4D})(t(1 -p_{4M}(t)), (6)
HUB

$P4_{s1\ldots n}$(t)= P_{4As1}(t)(1 - P_{4Ds1}(t)), …, (7)
home connected sensors 1 … n

$P4_s$(t) = [(p_{4S1}(t))(p_{4s2}(t)) … (p_{4sn}(t))][p_{4A}(t)(1 – p_{4D}(t))(1 -p_{4M}(t)], (8)
home sensors connect to HUB

$P4$(t) = p_{4A1}(t)(1 – p_{4D1}(t))(1 – p_{4M}t), (9)
HUB with attackers, defence and countermeasures

$P4$(t) = p_{HUBA1}(t)(1 – p_{HUBD1}(t))(1 – p_{HUBM1}(t)[($P2_{13}$(t) + $P3$(t) + [p_{5A}(t)(1 – p_{5D}(t))(1 – p_{5M}(t)] (10)
all in HUB

$P6$(t) = $p4$(t)(p_{AEDGE} (t))(1 – p_{DEDGE}(t)(1 – p_{MEDGE}(t)), (11)
EDGE with HUB, attackers, defence and countermeasures

$p7$(t) = [($p2_{13}$(t) + $p3$(t) + $p5$(t)][($p7$(t)(1 – $p7_A$(t))(1 – $p7_D$(t))(1 – $p7_M$(t))], (12)
phone, laptop or tablet connect to MEC router.

Tables 6 – 9 present the threats to different access network devices, which were defined with project specialists for each environment, segment and device. The author developed and made these definitions based on information from the NOC and SOC and on years of experience and insights into the development of these issues and the

safer solutions used in the auditing processes. The author was also involved in the development of the NOC and SOC systems. The author used information from (1) materials of the national cyber security centres; (2) VAHTI-instructions and Katakri 2015. Katakri is an audit tool for authorities and the recommendations; (3) regulations of the Finnish Transport and Communications Agency, Traficom; and (4) EU directives for security, TEMPEST and energy efficiency in the definitions.

TABLE 6. Smart Watch Threats

D	DESCRIPTION OF THE THREAT	EFFECT OF THE THREAT	EXISTING CONTROL	THREAT LEVEL 1 - 5	CONSEQUENCE 1 - 5	PROBABILITY	RECOMMENTED CONTROLS
- SW	SOFTWARE IS NOT REVISED, PROPRIETARY	GIVES POSSIBILITIES FOR MALWARE THROUGH SOFTWARE	ONLY IN SMART WATCH CONTROLS	3	3	0.6	USE REVISED SOFTWARE, TRUSTED MANAGEMENT SYSTEM IS IN USE
- SW	THE SUPPLY CHAIN IS NOT CLEAR	GIVES POSSIBILITIES FOR MALWARE THROUGH DEVICE	ONLY IN SMART WATCH CONTROLS	3	3	0.6	USE ONLY TRUSTED SUPPLIERS
- SW	SOFTWARE UPDATES	OLD SOFTWARE GIVES ATTACKERS POSSIBILITIES TO ATTACK	ONLY IN SMART WATCH CONTROLS	3	3	0.6	UPDATE
- SW	PROTECTIONS SYSTEMS	GIVES ATTACKERS POSSIBILITIES TO ATTACK	THERE ARE ANY PROTECTION MECHANISMS	4	4	0.8	NEW TYPE OF DEVICE ARCHITECTURE
- SW	ACCESS TO SMART PHONE	WIRELESS CONNECTION GIVES POSSIBILITIES TO ATTACK	WIRELESS CONNECTIONS ARE NOT PROTECTED	4	4	0.8	THE ENCRYPTION SYSTEM MUST BE INSTALLED
- SW	IDENTITY	IDENTITY CHECK IS NOT MADE IN A TRUSTED WAY AND ATTACK POSSIBILITES ARE THERE	THERE ARE NO CONTROLS FOR THOSE POSSIBILITIES	4	4	0.8	IDENTITY MUST BE VERIFIED OF SOFTWARE BASED ON ACCEPTED PROCESS, …
	..	..	..	..	..	..	..

Table 6 lists only the threats defined for that use case (Smart Watch Threats), but many other threats exist depending on the environment and the use case. A threat level of value 5 means the highest threat level against our systems and a consequence value of 5 means the highest value of what happens when this threat is realised. Other tables use the same values definitions.

Based on working group information, the attack probability is $pSW_A = 0.7$, and the defence probability is $pSW_D = 0.3$ in that case.

Before the smart watch device is audited, we also calculate the residual risks and threats. When an audit organisation is audited, they check to see if the architecture team's recommendations are sufficient to reduce the threats or not, and they make recommendations which must be done before the next audit.

TABLE 6. Smart Phone Threats

D	DESCRIPTION OF THE THREAT	EFFECT OF THE THREAT	EXISTING CONTROL	THREAT LEVEL 1 - 5	CONSE-QUENCE 1 - 5	PROBA-BILITY	RECOMMENTED CONTROLS
-SP	SOFTWARE IS NOT REVISED	GIVES POSSIBILITIES FOR MALWARE THROUGH SOFTWARE	ONLY IN SMART DEVICE CONTROLS	3	4	0.6	USE REVISED SOFTWARE, TRUSTED MANAGEMENT SYSTEM IN USE, TRUSTED SERVICE OPERATOR
-SP	THE SUPPLY CHAIN IS NOT CLEAR	GIVES POSSIBILITIES FOR MALWARE THROUGH DEVICE	ONLY IN SMART PHONE CONTROLS WITH ACCESS CONTROLS	3	4	0.6	USE ONLY TRUSTED SUPPLIERS, REVISED SOFTWARE, TRUSTED SERVICE OPERATOR
-SP	SOFTWARE UPDATES	OLD SOFTWARE GIVES ATTACK KERS POSSIBILITIES TO ATTACK	ONLY IN SMART DEVICE CONTROLS	3	3	0.6	UPDATE, TRUSTED SERVICE OPERATOR SERVICE IN USE
-SP	PROTECTION SYSTEMS	GIVES ATTACKERS POSSIBILITIES TO ATTACK	THERE ARE ANY PROTECTIONS MECHANISMS	4	4	0.8	NEW TYPE OF DEVICE ARCHITECTURE
-SP	ACCESS TO SMART WATCH AND HOME HUB	WIRELESS CONNECTION GIVES POSSIBILITIES TO ATTACK	WIRELESS CONNECTIONS ARE NOT PROTECTED	4	4	0.8	THE ENCRYPTION SYSTEM MUST BE INSTALLED
-SP	IDENTITY	THERE ARE MANY IOT DEVICES CONNECTED AND IT GIVES POSSIBILITIES TO ATTACKS	THERE ARE NO CONTROLS FOR THOSE POSSIBILITIES	4	4	0.8	IDENTITY MUST BE VERIFIED OF SOFTWARE BASED ACCEPTED PROCESS
-SP	SMART PHONE IS WIRELESSLY CONNECTED TO MOBILE NETWORKS AND ACCESS DEVICES	IT IS OPEN FOR ATTACKS IN WIRELESS CONNECTIONS	NO PROTECTION AT NETWORK PROTOCOL LEVELS	4	4	0.8	NEW TYPE OF DEVICES, HARDENING OF DEVICE, AUTOMATIC CHECKING OF DEVICE
	...	...	...	...	...	...	...

Table 7 lists only the threats defined for that public use case, but there are many other threats depending on the environment and the use case. Based on the working group information, the attack probability is $pSP_A = 0.75$, and the defence probability is $pSP_D = 0.25$ in that case.

Before this smart phone was audited, we also calculated the residual risks and threats. When an audit organisation is audited, they check whether the residual risks recommendations are sufficient to reduce the threats and indicate which recommendations must be done before the next audit. Smart phones are audited as one device and recommendations are given about in which environments they can be used.

TABLE 7. Home Hub (Room Hub) Threats

D	DESCRIP-TION OF THE THREAT	EFFECT OF THE THREAT	EXISTING CONTROL	THREAT LEVEL 1 - 5	CONSE-QUENCE 1 - 5	PROBA-BILITY	RECOMMENTED CONTROLS
-HH	SOFTWARE IS NOT REVISED	GIVES POSSIBILITIES FOR MALWARE THROUGH SOFTWARE	ONLY IN USE HOME HUB CONTROLS	4	4	0.8	USE REVISED SOFTWARE, TRUSTED MANAGEMENT SYSTEM IN USE
-HH	THE SUPPLY CHAIN IS NOT CLEAR	GIVES POSSIBILITIES FOR MALWARE THROUGH DEVICE	ONLY HOME HUB ONTROLS	3	4	0.6	USE ONLY TRUSTED SUPPLIERS
- HH	SOFTWARE UPDATINGS	OLD SOFTWARE GIVES ATTACK KERS POSSIBILITIES TO ATTACK	ONLY IN SMART DEVICE CONTROLS	4	3	0.8	UPDATE AND USE SERVICE OPERATOR'S SERVICE
-HH	PROTECTION SYSTEMS	GIVES ATTACKERS POSSIBILITIES TO ATTACK	THERE ARE ANY PROTECTIONS MECHANISMS	4	4	0.8	NEW TYPE OF DEVICE ARCHITECTURE OR SERVICE OPERATOR SERVICE, …
-HH	ACCESS TO SMART PHONE AND TO EDGE ROUTER	WIRELESS CONNECTION GIVES ATTACKERS POSSIBILITIES TO ATTACK	WIRELESS CONNECTIONS ARE NOT PROTECTED, BLUETOOTH	4	4	0.8	THE ENCRYPTION SYSTEM MUST BE INSTALLED, …
-HH	IDENTITY	POSSIBLE TO CONNECT OTHER DEVICE TO SAME HOME HUB	THERE ARE NO CONTROLS FOR THOSE POSSIBILITIES	4	4	0.8	CONNECTED DEVICE IDENTITY MUST BE VERIFIED, EXAMPLE SOFTWARE BASED ACCEPTANCE PROCESS, …
	…	..	..	..	..	..	..

Table 8 lists only the threats defined for that public use case, but many other threats exist depending on the environment and use cases. Based on working group information, the attack probability is $pHH_A = 0.8$, and the defence probability is $pHH_D = 0.2$ in that case.

Before auditing this Home Hub (Room Hub), we also calculated the residual risks and threats. When an audit organisation is audited, they check to see whether residual risks recommendations are sufficient to reduce threats and make recommendations to perform before the next audit for final acceptance.

TABLE 8. Edge Router Threats

D	DESCRIPTION OF THE THREAT	EFFECT OF THE THREAT	EXISTING CONTROL	THREAT LEVEL 1 - 5	CONSEQUENCE 1 - 5	PROBA-BILITY	RECOMMENTED CONTROLS
- ER	SOFTWARE IS REVISED	GIVES SMALL POSSIBILITIES FOR MALWARE THROUGH SOFTWARE	SERVICE OPERATOR CONTROL SYSTEMS	1	2	0.1	USE REVISED SOFTWARE AND MANAGEMENT SYSTEMS AND UPDATE THEM REGULARLY
- ER	THE SUPPLY CHAIN IS CLEAR	GIVES ONLY SMALL POSSIBILITIES FOR MALWARE THROUGH SYSTEM	SERVICE OPERATOR CONTROL SYSTEMS, CMDB	1	2	0.1	IPS-, IDS-, SIEM SYSTEMS IN USE
- ER	USED EDGE ROUTER IS INSIDE A PROTECTED ROOM	THIS GIVES SMALL POSSIBILITIES TO ATTACKERS	ONLY AUTHORISED PERSONS ARE ACCESSIBLE	1	2	0.1	ACCESS CONTROL AND ALARM SYSTEMS
- ER	ACCESS TO SMART HUB	USE ONLY FIXED CONNECTION AND GIVES SMALL POSSIBILITIES TO ACCESS OUTSIDE	CONNECTIONS ARE PHYSICALLY PROTECTED AND	1	2	0.1	FIXED CONNECTIONS MUST NOT ALLOW OUTSIDE CONNECTIONS
- ER	EDGE ROUTER IDENTITY	ATTACKERS MAY USE ANALYSIS TOOLS TO ACCESS DEVICE	OPERATORS CONTROL THE SYSTEMS WITH THEIR CONNECTED DEVICES	1	2	0,1	THE SERVICE OPERATOR MUST IDENTIFY THE DEVICE BEFORE USE, CMDB
	..	..	..	..	..	..	..

Table 9 lists only the threats defined for that public use case, but many other threats exist depending on the environment and use case. Based on working group information, the attack probability is $pER_A = 0.1$, and the defence probability is $pER_D = 0.8$ in that case.

Before the Edge Router systems are audited, we calculate the residual risks and threats. When an organisation is audited, they check to see whether the residual risk recommendations are sufficient to reduce the threats and make recommendations about what must be done before the next audit and final acceptance. The Edge Router auditing is part of supply chain auditing process or access networks auditing process.

$P1_1 = 0.7x(1 – 0.3) = 0.49$, Smart Watch
$P2_1 = 0.49 \times 0.75 \times (1 – 0.25) = 0.27$, Smart Phone with Smart Watch
$P3_1 = 0.27 \times 0.8 \times (1 – 0.2) = 0.173$, HUB with Smart Phone and Smart Watch

We have three different devices connected to each other and to the HUB, In Figure 17, which all may have vulnerabilities that allow attackers to attack our system in this case.

The author uses the same type of tables, definitions and calculations in Chapter 5 to conduct a threat analysis for the access networks in a hospital environment. The same calculations can be used for smart cities in the Arctic regions and countries in Europe, Russia and Asia to make cyber threat calculations and perform an analysis.

The threats in tables 6 – 9 defined in working group which included professional peoples in different ministries. The tables contain the entities, descriptions of the threats to consider, the existing controls, the related threat/risk level and consequence level, probability and recommended controls. In the future, it is evaluated how the risk is treated, what are the recommended controls and remedies with its responsible persons (including organisations). Finally, the equivalent values and checkpoints after the remedies are estimated. Separate tables can be created for the cyber threats and risks, and columns can be added as needed depending on the issues being viewed and related contexts. Based on the QFD model, we can include the system life cycle cost calculations from their acquisition to rejection as well as the purchase costs, annual maintenance costs, software and hardware upgrade costs, and rejection costs. Systems and services can also be compared using the QFD model to choose the most ecological and energy-efficient, but also the most cost-effective options. However, cost analyses and comparisons are not made in this example.

2.10 Answers to research the questions, conclusions and future work

Answer to the research questions:

RQ 1: The EA framework is needed to develop architectures in service, information and communications system and environments. The EA framework provides a clear path for determining which architectures are needed in the environments of smart cities and smart societies for the citizens.

RQ 1.1: The QFD model was used to find the dependencies between different information systems, applications and services and to identify the different data centre layers, requirements and co-operations needed between the different organisations, security layers and system life cycle functions.

RQ 1.2: Considerable work is needed to develop the required architecture in smart cities and smart societies: information architecture, integrations architecture, target architecture, security architecture, and security issues. Service chains must be checked against the architectures to ensure no risks are present.

RQ 1.3: Appendices 1 and 2 show the calculations of the power consumption in data centres and communication networks devices and systems that have not been virtualised. Data centres, communication systems and device virtualisations are the most important ways to significantly reduce energy consumption while reducing CO_2 emissions. As the next phase of virtualisation is coming to our information systems, with zero-energy solutions for our communications systems and IoT devices, more energy efficient solutions are required.

RQ 1.4: The author used attack tree models and the QFD model to calculate cyber threat probabilities. However, the needed requirements must be defined, and architectures must be developed and done before we can analyse our environments and make threats calculations.

Conclusion

A threats analyses is difficult to conduct because the number of IoT and sensor devices connected to telecommunication networks is increasing exponentially. An analysis of each connected IoT device or sensor is time-consuming and the results may be inadequate in some respects. Technical developments are proceeding at an accelerating pace and the importance of analysing individual components needs to be recognised. Even though the dependencies, dependency analyses, and threat assessments and analyses could be done sufficiently comprehensively in some areas. It is essential that the threat assessments and analysis of future societal services are made with the support of computer programs and machine learning because it is faster than human to does. If the vulnerability of the OSI layers, and the various vulnerabilities associated with the various protocols in use are added to this whole the number of issues to be verified is increasing. The inherent defects and vulnerabilities of encryption solutions and cryptographic network solutions must also be analysed. In the future, the design and development of the systems will need to take into account the increasing amount of energy efficiency and ecological requirements.

Future Research

Future research should examine the functionality of the virtual access network services and the terminals that use them in various attack situations. It is important to research, for example, remote medical care systems, rescue authorities' systems and security authorities' systems. Figure 8 demonstrates the complex structures of the active nodes of ecosystems and information flows in hyper-connected environments. As we can see, the operations of most computer systems in critical situations is extremely challenging because there are many networks connections and systems which are working together. With the addition of cyber-attackers waiting for opportunities to enter the networks and services, we are faced with many challenges.

Another important research topic is the use of machine learning in the analyses to speed up the work and provide opportunities to identify vulnerabilities and fix them quickly. As a result, security measures could quickly target the right location to prevent potential penetration into multiple networks and services, thereby preventing or minimising the effects of attacks.

The third research topic is the use of artificial intelligence (AI) for real-time tracking and analysis at different GW points to analyse the network threats and security and systems management.

Another area of research involves developing a quantum encryption system that could be used for wireless networks and services in the future.

CHAPTER 3. UNDERSEA OPTICAL CABLE NETWORK AND CYBER THREATS.

This chapter is based on publication PII entitled 'Undersea Optical Cable Network and Cyber Threats' and additional earlier materials and works by the author developing submarine optical cables for a Finnish cable organisation and for security authorities. As part of a group, the author also developed optical cables for the tactical network needs.

The author completed her master's thesis ('DWDM Technology in Communications Networks') and special work ('WDM -Technology in N-ISDN- Subscriber Networks') at the Helsinki Technical High School, Otaniemi (Hummelholm, DWDM-tekniikkaa, 12.6.2000) (Hummelholm, WDM-tekniikkaa, 1997-

1998). The author has also developed research submarine optical cable systems' technologies, risks and threats in the Arctic region (PII, PIII and PV).

3.1 Introduction

Figure 20 shows how different parts of the world are currently connected to each other by submarine optical cables.

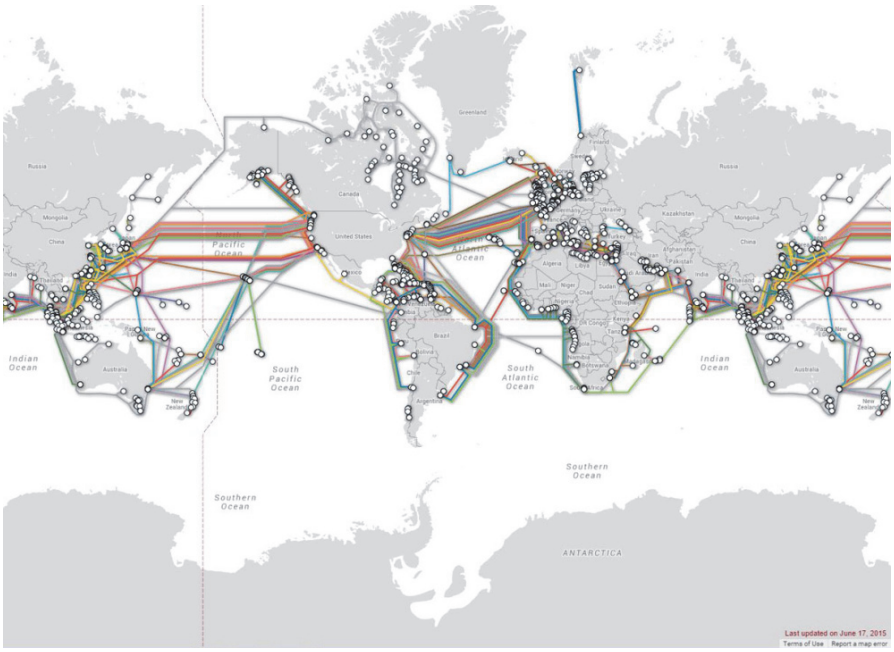


FIGURE 20. Map of the worldwide undersea submarine cable (Reddit, 30.8.2017).

These cables are concentrated in the southernmost seas of the globe, and the terminals for submarine optical cables are located in areas where it is relatively easy to build cable endpoints, including cable communication and energy systems. Each country has its own inside fibre network that connects the cities and countryside (see Figure 22).

Currently, as the submarine optical cable route between Asia and Europe is long, the undersea submarine optical cable system could break down. Terrorists could deliberately damage the cables, cyber attackers can penetrate them and natural disasters also pose a risk. These and many other risk factors necessitate the design of new submarine optical cable routes between Asia and Europe to ensure secure communication links between these areas. Figure 21 is a general overview of the Arctic Optical Cable Systems, which combines different regions of Europe, the Western parts of Russia, the Siberian Russian regions, areas in the Russian Far East, smart cities in Japan and the border areas of China.

FIGURE 21. The Arctic connect cable system (Joensuu, 13.2.2018)

An increased communication capacity and many new contact points will be needed in the future to satisfy the data transfer needs of users, businesses organisations and governments in these north areas. These areas thus require proper and reliable communication links to be able to communicate and to use the services offered by the rest of the world. Regional development and joint operations in these northern areas require communication links. This new connection will give people in the area real-time access to existing digital services in their home country, which they can use to communicate with their friends, either locally or worldwide.

3.2 Objective and organisation of the chapter

This study aims to develop a model that can be used to conduct threat assessments, compare threats and facilitate a threats analysis in ocean environments, particularly in the Arctic region. In addition to the technical design criteria, the model should address different types of threats such as natural threats, accidents, terrorists and cyber-attacks. The results obtained through the model will facilitate the design and implementation of architectural solutions. The implemented model will help to improve the assessment of the threat scenarios for future submarine optical cables system environments and their impact probabilities. The study utilises the operating environment introduced in Figure 21, which groups different parts of continental services and infrastructure together. Threat research can be done in different segments of submarine optical cables to assess the types of threats to those segments. The political and commercial aspects of the Arctic region have not been included in the study. The Arctic's communication networks, submarine optical cable communications networks, and data centres and services are effectively one entity through which all future services will be implemented; in the future, these services will work together between the different continents. This integration is accelerating at all levels of activity, in each region and all segments both horizontally and vertically. The nature of these environments will further complicate the threat estimates of these kinds of ecosystems.

Section 3.3 presents the ecosystems and future operating environments of the telecommunication networks, data centres and the submarine optical cable communications networks on a general level. Section 3.4 describes the natural threats, accidental threats, cyber-threats and dependency analyses which are used to conduct a threats analysis for the submarine optical communications networks and network infrastructures, and the services it provides. Section 3.5 describes the development of the threats analyses, and Section 3.6 presents the conclusions, a solution model for security and future work.

3.3 The following research questions are addressed in Chapter 3

RQ 2. What are the attack possibilities in submarine optical cable systems?

RQ 2.1. How can we ensure that communication systems between continents are sufficiently secure to use them daily in our services?

3.4 Description of the future operating environment and technology

When the Arctic Optical Cable System is installed, European and Asian Smart societies of the future will be connected to each other by a new route. The estimated length of the incoming connection of the Arctic Optical Cable's route is about 18,000 - 20,000 km (Figure 21), which sets a number of requirements for the design and implementation of this submarine's optical cable system. Figure 23 presents an overview of the Arctic connect cable system, which author was examined.

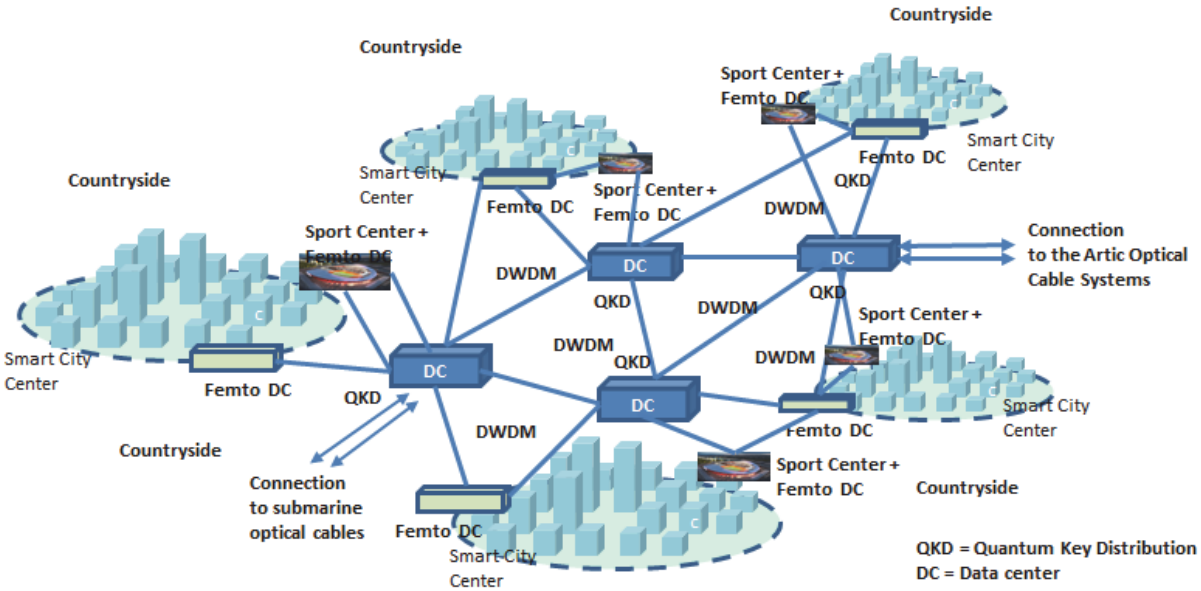


FIGURE 22. Smart cities in the future environment, top level principle.

The Arctic optical cable route will likely be of interest to hackers, terrorists, cyber attackers and state actors because it will contain a lot of information being transferred between Europe and Asia.

Because of the importance and the length of the route, the technical values and requirements that affect the design of the system must be investigated and the result utilised in both the design and maintenance of the system. When we perform system deployment measurements, those values can be used later to detect the smallest changes in the system and identify any attempts to attack the system. These problems or defects may be caused by natural forces, construction works at sea, terrorists or cyber attackers. All such phenomena cause lesser or greater changes in the measured values associated with the operation of the system. However, not all situations can be obtained from identifiable numerical data that can be detected by management and control devices, for example, the tapping of submarine optical cable results in less than a 2% loss of optical signal power and it is thus not so easily correctly detected by existing technologies. Consequently, even the smallest deviations must be reviewed and analysed. For this reason, we must identify the factors affecting fibre quality that result from the properties of the fibres themselves. This is important to know and take into consideration because it affects the construction of a connection in a number of ways, such as the wavelength and bandwidths supported by the fibres, the distance between optical amplifiers (OAs) from each other and the optical signal levels to be used. As this is also a long-term investment and the submarine optical cable may be in use for more than 25 years, the evolution of technology must also be taken into consideration to anticipate early and timely updates and changes to the systems and equipment. In addition, when transmission speeds are increased in the wavelength by the fibres, there will still be a few boundaries that we can no longer exceed using the current technology. These are the physical limits of single-mode fibre (SMF) and two other limits of optical communications – the Fibre-launched power limit and the Non-linear Shannon limit (Yutaka Miyamoto, Ryutaro Kawawura, June 2017).

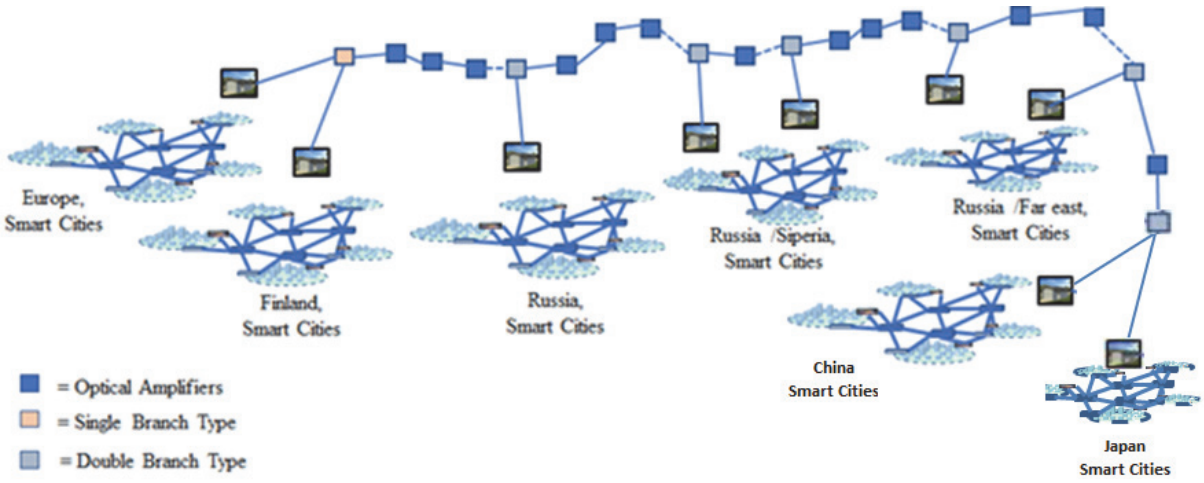


FIGURE 23. Overview of the Arctic connect cable system.

3.4.1 The evolution of technology

Regarding the life cycle of the optical cable system, we must understand at least in part the technical evolution that will occur in optical telecommunication technology and how that will affect these long connections. The optical channel capacity cannot be

increased indefinitely, despite the wide optical bandwidth available in the optical range. We can calculate the optical channel capacity that can be achieved (Chesney, 2016). We can use Shannon's definition of the upper limit for transmission capacity (or spectrum efficiency) that can be transported in the transport channel as $C = B \log (1 + SNR)$, with C being the capacity in bit/s, B the bandwidth in Hz and SNR being the signal-to-noise ratio. We can also define the single-sided optical noise power spectral density as $S_n = hv/2$, where $h = 6.63 \times 10^{-34}$, Js is the Planck value, hv is the proton energy 10^{-19}J, and the minimum average optical noise power $P_N = (hv/2) B_0$ is proportional to the bandwidth.

Therefore, the optical channel capacity, treated in terms of the optical field, is

$$C = B_0 \mathrm{Log}_2 (1 + 2P_s / hvB_0). \quad (1)$$

Since the life cycle of a fibre optic cable to be built is long, up to at least 25 years, we must know what will occur in the technical evolution of optical telecommunication technology and the way in which we must take care of those things in relation to these long connections. In Figure 6, we can see which directions the evolution is heading. But the optical channel capacity cannot be increased indefinitely, despite the wide optical bandwidth available in the optical range. We can calculate the possible optical channel capacity (Miyamoto Yutaka, Kawawura Ryutaro, NTT Technical Review, 6 June, 2017).

We can see also in Figure 24 the physical limits of single-mode fibre (SMF). There are also two other limits for optical communications: the Fibre-launched power limit and the Non-linear Shannon limit. When designing a telecommunications system based on long-distance optical undersea cables, we must take very strictly into account those limiting factors relating to optical fibres. We must also take into account the features and operational models of these optical undersea cable systems parameters in practical networks to obtain more accurate information about the functions of the existing system so that we can detect possible intrusion attempts. Since more capacity is needed per fibre pair, a new optical signal band, the L-band, is introduced. The C and L bands, which form the basic band of future long-distance optical networks (ITU-T Manual, 2009), provide a challenge to network designers to find an OA with sufficient bandwidth. In C-band, there are 80 optical channels and L-band has 80 optical channels (Figure 25). If we transmit 100 Gbit/s through one wavelength, this means, for example, that we would have 80 X 100 Gbit/s capacity in use in this kind of network.

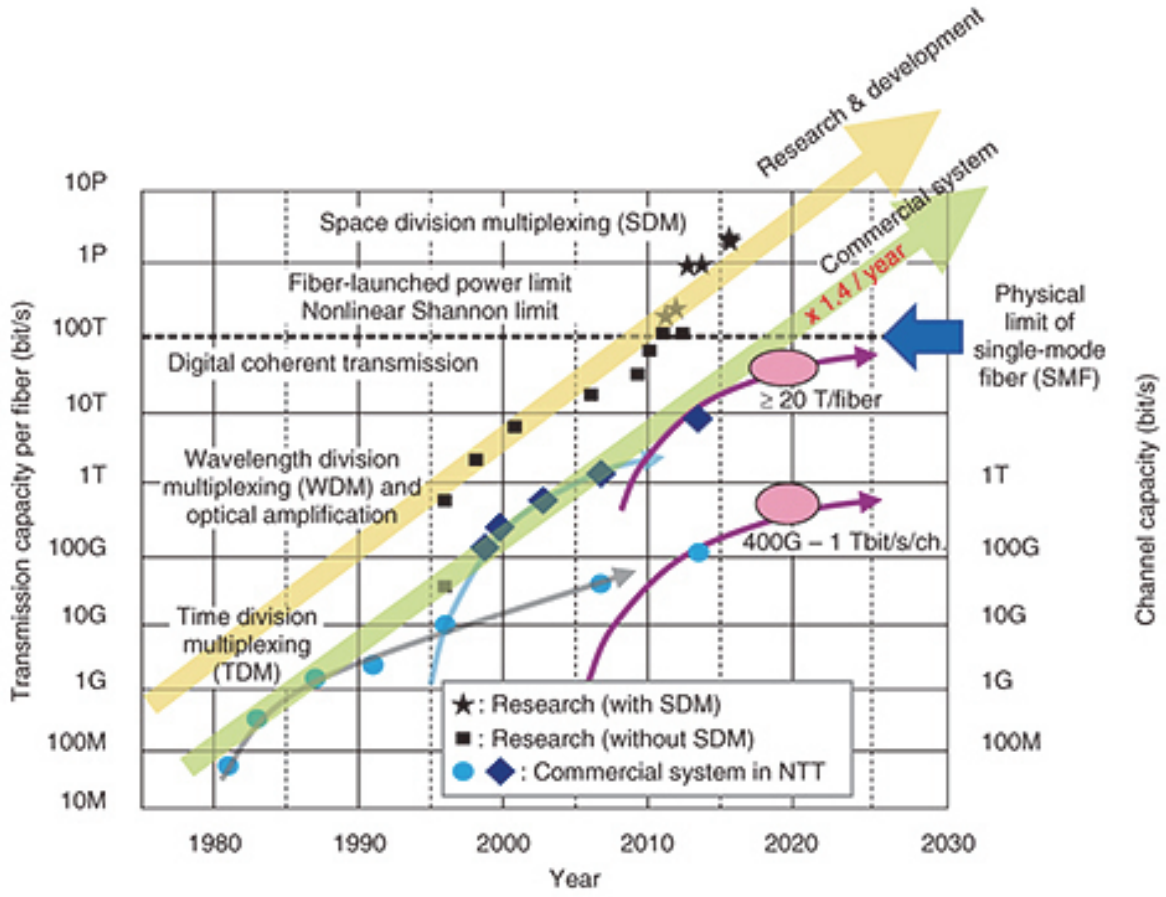


FIGURE 24. Evolution of a high-capacity optical transport network (OTN).

Since fibre band attenuation in L-band is reasonable low value, it is useful to use for high-capacity optical transport network (OTN). Network designers thus need to find an OA which has enough capacity to work with C-band and L-band at the same time as one amplifier.

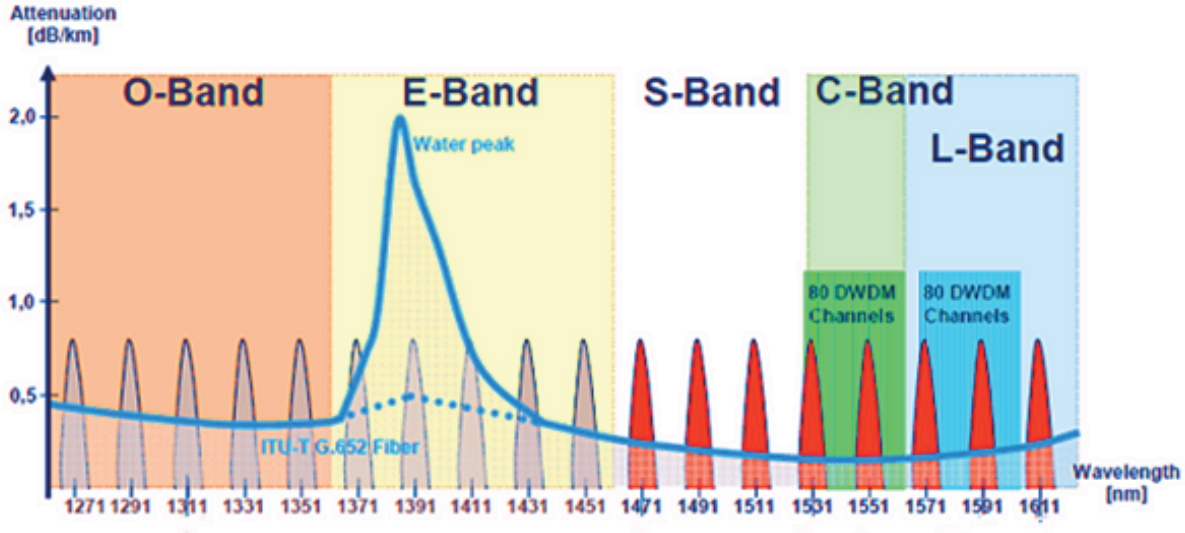


FIGURE 25. High-capacity OTN optical bands (Cheer, 2015).

3.4.2 Long distance submarine optical systems

By 2015, a mature product had the capacity of 100 Gbit/s per optical wavelength. Since then ongoing development has continued to find new solutions aimed at increasing wavelength capacity per optical wavelength. As a result of this development, capacities of 200 Mbit/s and 400 Mbit/s are now available. To obtain transmission rates of 100 Mbit/s or more in submarine optical cables, it would be necessary to install OAs at about 50 km intervals. This distribution would provide sufficient quality of service across continents.

3.4.3 The primary principles of the installation

A submarine optical cable system of 18,000 km in length will be installed in the Arctic region (Figure 21). There will be few branching points with connections to the continent (Figure 23). Each cable landing station will be built in the same way. The difference between them will be only how the submarine's optical cables can be brought to the station, which depends on the beach area.

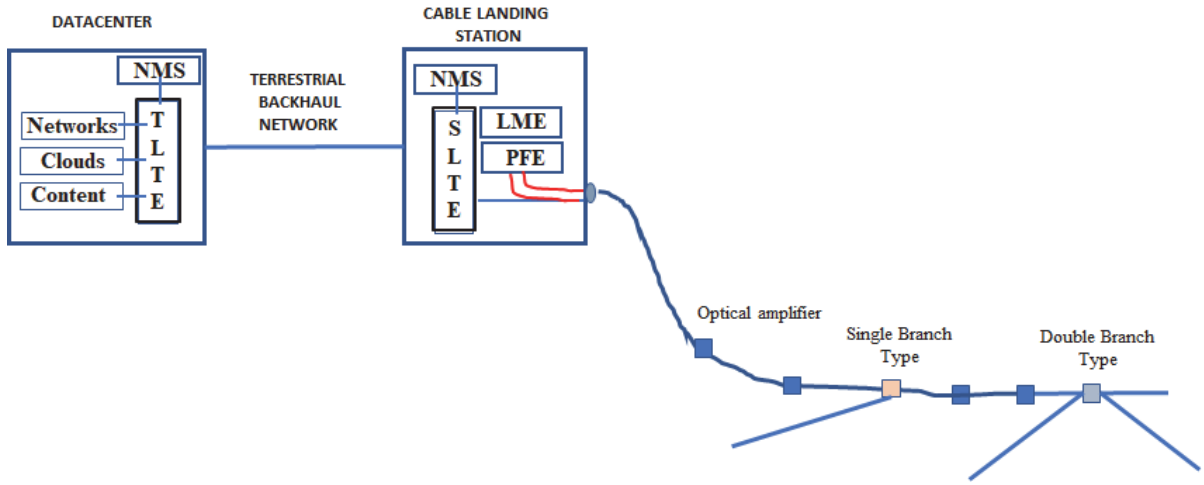


FIGURE 26. Subsea optical cable system architecture with cable landing station and data centre.

Subsea optical cable system architecture (Tara, 2015) (Ye Yincan, Jiang Xinmin, Pan Guofu, Jiang Wei, 2018).

In Figure 24, the Data Centre NMS means Network Management System, and TLTE means Terrestrial Line Terminal Equipment. Cable Landing Station NMS means Network Management System, LME means Line Monitoring Equipment, PFE means Power Feed Equipment, SLTE means Submarine Line Terminal Equipment.

The main reason that the distance between OAs is only 50 km is due to the dispersions and non-linear properties of the optical cables, the characteristics of the OAs, the noise levels and the characteristics of the fibre. As the modulation techniques of optical data transfer become more complex, we must design systems even more carefully. The distance between the amplifiers is optimised based on the usability and quality of the services. Performance and cost optimisation are expressed in terms of cost efficiency, €/bitti/hz. These systems also need electrical energy. Energy input to the

system can be made of one or more earth points, taking the energy supply protection into account in case of damage to the cable systems.

3.5 Designing submarine optical cable systems

To achieve the required usability and quality requirements for very long optical undersea cable connections, the following factors in this chapter 3.5 need to be considered. We also need to understand the parameters and impairments of optical submarine cables to determine whether there are any faults in the cable connection and links or whether hackers or cyber attackers are connected to the cable in one way or another to gather information or even to spy. We must first look for factors which affect the fibre quality.

3.5.1 Attenuation

Attenuation values varies between different wavelength bands of 800, 1300 nm and 1550 nm and is smallest in the 1550 nm band, where it is about 0.2 db/km or smaller.

Several factors can cause attenuation, but it is generally categorised as either intrinsic or extrinsic. Intrinsic attenuation is caused by substances inherently present in the fibre, and extrinsic attenuation is caused by external forces such as bending. Extrinsic attenuation may be caused by macro or micro bending as both raise the fibre attenuation values. This bending mechanism means it can be used in cyber-attacks to obtain information from optical cables without anybody noticing.

3.5.2 Dispersions

Rayleigh Scattering

- As light travels in the core, it interacts with the silica molecules in the core. Rayleigh scattering is the result of these elastic collisions between the light wave and the silica molecules in the fibre. Rayleigh scattering accounts for about 96% of attenuation in optical fibres.

Chromatic dispersion

- Chromatic dispersion is the spreading of a light pulse as it travels down a fibre. Light has a dual nature and can be considered from the perspective of an electromagnetic wave as well as a quantum perspective. This allows us to view it in the form of both waves and quantum particles.

Polarisation Mode Dispersion (PMD)

- PMD is caused by asymmetric distortions to the fibre from a perfect cylindrical geometry. The fibre is not truly a cylindrical waveguide, and it can be best described as an imperfect cylinder with physical dimensions that are not perfectly constant. The mechanical stress exerted upon the fibre due to extrinsically induced bends and stresses caused during cabling, deployment,

splicing and the imperfections resulting from the manufacturing process are the reasons for the variations in the cylindrical geometry.

Optical Signal-to-Noise Ratio (OSNR)

- OSNR specifies the ratio of the net signal power to the net noise power and thus identifies the quality of the signal. Attenuation can be compensated for by amplifying the optical signal. However, OAs amplify the signal and the noise. Over time and distance, the receivers cannot distinguish the signal from the noise, and the signal is completely lost.

3.5.3 Impact of non-linearity

Nonlinear characteristics include Self-Phase Modulation (SPM), Cross-Phase Modulation (XPM), Four-Wave Mixing (FWM), Stimulated Brillouin Scattering (SBS) and Stimulated Raman Scattering (SRS).

FWM

- FWM can be compared to the intermodulation distortion in standard electrical systems. When three wavelengths (λ1, λ 2 and λ 3) interact in a nonlinear medium, they give rise to a fourth wavelength (λ 4), which is formed by scattering of the three incident photons, producing the fourth photon. This effect, known as FWM, is a fibre-optic characteristic that affects WDM systems.

SPM

- SPM is primarily caused by the self-modulation of the pulses. Generally, SPM occurs in single-wavelength systems. At high bit rates, however, SPM tends to cancel dispersion. SPM increases with high signal power levels.

XPM

- XPM is a nonlinear effect that limits system performance in WDM systems. XPM is the phase modulation of a signal caused by an adjacent signal within the same fibre. XPM is related to the combination of (dispersion/effective area) and results from the different carrier frequencies of independent channels, including the associated phase shifts.

SBS

- SBS is caused by the acoustic properties of photon interaction with the medium. When light propagates through a medium, the photons interact with silica molecules during propagation.

SRS

- When light propagates through a medium, the photons interact with silica molecules during propagation. The photons also interact with themselves and cause scattering effects, such as SRS, in the forward and reverse directions of propagation along the fibre. This results in a sporadic distribution of energy in a random direction.

3.6 Long distance cable systems attenuation calculations

The power budget table should compute margins to be considered as a minimum requirement for the system at beginning of life (BOL). These margins should be expressed in terms of a Q factor value. The contractors should provide, as a minimum, the values of the parameters used to compute the power budget and specify all necessary complementary relevant information, for instance, the use of any optical polarisation scrambling or phase modulation to minimise the polarisation effects or nonlinear effects. Table 10 presents an example of a possible power budget template (ITU-T G.977).

TABLE 9. ITU-T G.977 Power Budget Table of a Submarine Optical Cable Transmission Digital Line Sections (DLS)

	Parameter		BOL Q in dB	EOL Q in dB
1	Mean Q value (from a simple SNR calculation)		9.5	9.3
1.1	Propagation impairments due to combined effects of chromatic dispersion, non-linear effects, FWM effects, SRS effects, etc.		- 1.8	- 1.6
1.2	Gain flatness impairments		-	-
1.3	Non-optimal optical pre-emphasis impairment		-	-
1.4	Wavelength tolerance impairment		- 0.5	- 0.5
1.5	Mean PDL penalty		-	-
1.6	Mean PDG penalty		-	-
1.7	Mean PMD penalty		-	-
1.8	Supervisory impairment		- 0.2	- 0.2
1.9	Manufacturing and environmental impairment		- 0.5	- 0.5
2	Time-varying system penalty (5 sigma rule)		- 0.5	- 0.5
3	Line Q value (1-1.1 to 1.9-2)		= 6.0	= 6.0
4	Specified TTE Q value (back-to-back)		17.1	17.1
5	Segment Q value (computed from 3 and 4)		= 5.7	= 5.7
5.1	BER corresponding to segment Q without FEC		$2e^{-2}$	$2e^{-2}$
5.2	BER corresponding to segment Q with FEC		< $1e^{-13}$	<$1e^{-13}$
5.3	Effective segment Q value with FEC		> 17.3	> 17.3
6	Q limit compliance with [ITU-T G.826] or [ITU-T G.8201] after FEC		5.0	5.0

7	Repair margin, component- and fibre-ageing penalty, pump(s) failure penalty, non-optimal decision threshold		-	+0.7
8	Segment margins		+0.7	0.0
9	Unallocated supplier margin			0.0
10	Commissioning limits		= 5.7	

Abbreviations:

BER = Bit Error Ratio	PDG = Polarisation-Dependent Gain	Q = Quality factor
BOL = Beginning of Life	PDL = Polarisation-Dependent Loss	TTE = Terminal Transmission Equipment
EOL = End of Life	PMD = Polarisation Mode Dispersion	

Table 8 shows a typical power budget table of a 100 X 100 G 10,000 km DLS system. The table is based on recommendation ITU-T G.977 and Table A.1 there.

The table has two columns, the first dedicated to the BOL conditions and the second to the end of life (EOL) conditions.

3.7 Natural threats, accidental threats and cyber threats

In addition to the technical design criteria, we also need to take into account the various types of threats that will be encountered such as natural threats, accidental threats and cyber or malicious threats. The type of threat can contribute to prolonging the cable routes or partial routes and even altering the originally planned routes.

Natural threats include threats such as shark attacks, earthquakes, landslides, volcanic, eruptions, tsunamis, icebergs, sea currents and storm winds. Accidental threats can be caused by everyday work at sea, such as fishing, dragging an anchor and dredging and can damage submarine optical cables, threatening their level of performance. We also need to consider other potential threats since the submarine optical cable routes are long. Many countries have the ability to join (tap) fibre optic cables to collect the information being transmitted therein. In every situation, we must always be on the lookout for opportunities to hack into or launch cyber-attacks on submarine optical cables – whether by 'tapping' the lines or other methods such as side channel attacks or side channel spying.

3.7.1 Fibre optic networks and tapping

There are three main methods to 'TAP' optical cable systems: the splice method, the splitter or coupler method, and the non-touching method. The splice method, which involves disconnecting the fibre and installing a Y-bridge, is the easiest way to get information from a fibre. Devices are also used to service network or branching connections. The splitter/coupler method involves using a device to bend the fibre slightly (Figure 27). When the fibre is bent, light escapes from the fibre. With today's modern receivers 1%-2% of optical power is sufficient to receive the complete signal and read the data. When using this method, there is no link interruption and there are only

quite small attenuation changes in the link. When we get signals from fibre, we must use transceivers or media converter to get Ethernet or fibre optical channel signals out from the fibres for our analyses.

When we receive signals from the fibres, we can use communications analysers, protocol analysers or other analysers to view the data transmitted in the fibres and to collect all relevant information. When hackers and cyber attackers tap into the optical fibres and use communications analysers and protocol analysers to analyse all information being transmitted through the fibres, they can collect all non-encrypted information quite easily from those fibres (Figures 28 and 29).

The third method is the non-touching method in which sensitive photo detectors catch a minimal amount of light which radiates naturally from the cable.

When the author was involved in the fibre optic cable development project, they tested factory splices to see how they appear in Optical Time Domain Reflectometer (OTDR) measurements on the actual optical fibres in use. The tapping method (Figure 27) was also tested for the presence of excess connections in the cable. The tapping event was difficult to detect because in DWDM technology, the terminals automatically adjust their gain levels according to the fibre portion attenuation to the correct settings.

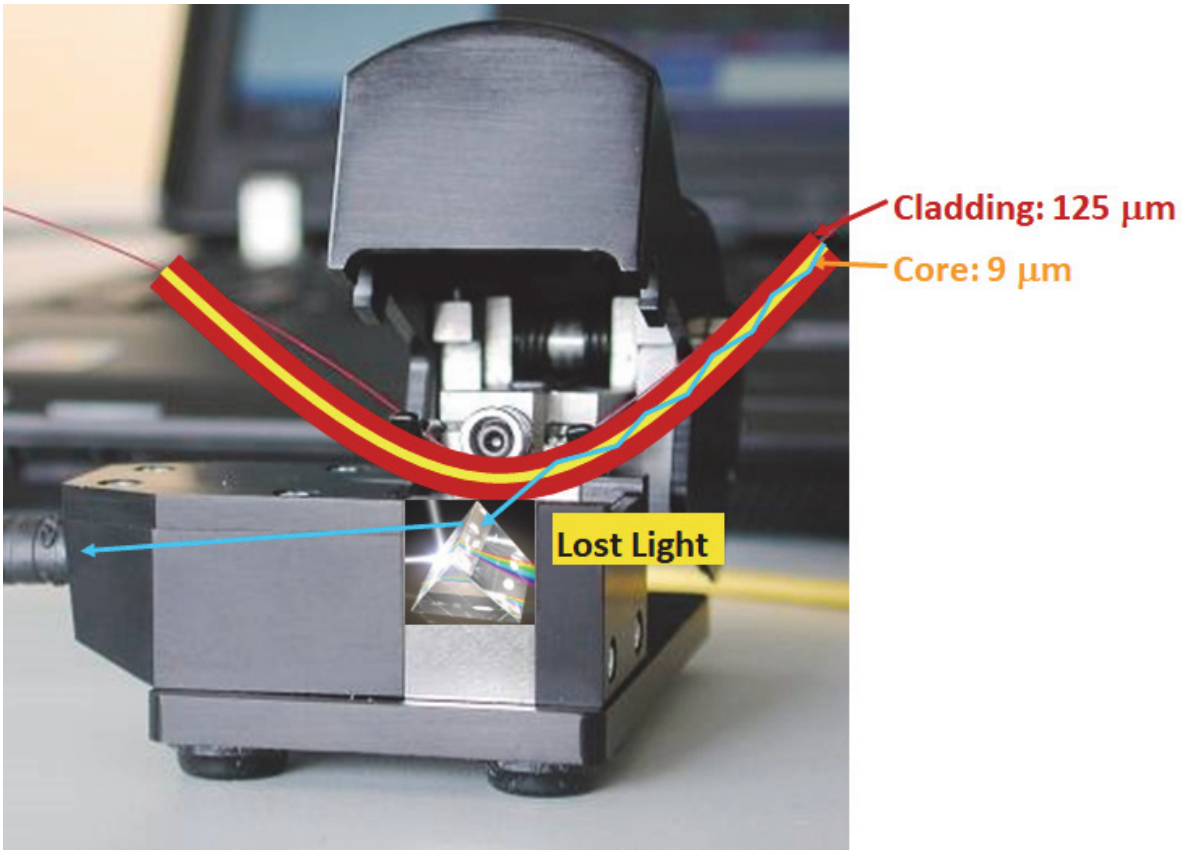


FIGURE 27. Fibre bending system in tapping.

The type of undersea cables chosen depends on the depth of the sea and the vicinity of the coast in the areas where the above-mentioned threats exist. If we consider the opportunities for cyber attackers to join to the optical cable, it would be easiest to penetrate the cable exactly where the cables' armour layers are thinnest. This also means that the attacker must be able to operate deep below the sea level. In practice, only a few large states have the capabilities to do this. When considering this planned undersea optical cable system, with a length of 18,000 km, cyber attackers will be able to connect to undersea optical cables after each OA, which is deep underwater.

3.7.2 Optical cable systems in use

Next, we consider a submarine optical cable system based on the ITU-T Recommendation (ITU-T, G.709/Y.1331) (ITU-T, G.971) (ITU-T, G.977 (01/2015)), which is divided into a land section, an underwater section and a second land section. The underwater section has the necessary branching equipment. An 18,000-km long submarine optical cable system requires power feed equipment (PFE).

We also need different types of OTDR to certify the performance of new fibre optic links and detect problems in existing fibre links. It is important to use a measurement system such as a Coherent OTDR (COTDR) for high capacity systems because in 18,000 km submarine optical cable systems, we would use different types of fibre cables to compensate for the dispersion phenomena. This dispersion compensation systems also means that when there are considerable cable branching and continued points, make it difficult to find the smallest deviations in the parameters. Submarine optical cable systems management and control systems are most critical systems. To identify security challenges in long distance optical cable systems, we must consider OTN framing and rates (Figure 28) and the OTN and OSI layer model (Figure 29).

Currently, few encryption technologies are in use for optical signals. Figure 29 shows where the client signal is seen in the OTN and how the header areas of the different layers are placed in relation to the client signal (ITU-T, G.709/Y.1331). Figure 29 more precisely portrays the information a cyber attacker could access and use if we do not encrypt these signals. For example, they can change the Reconfigurable Optical Add-Drop Multiplexer (ROADM) routing in whatever way they want, and either disrupt traffic or drive traffic to a desired connection point for analysis.

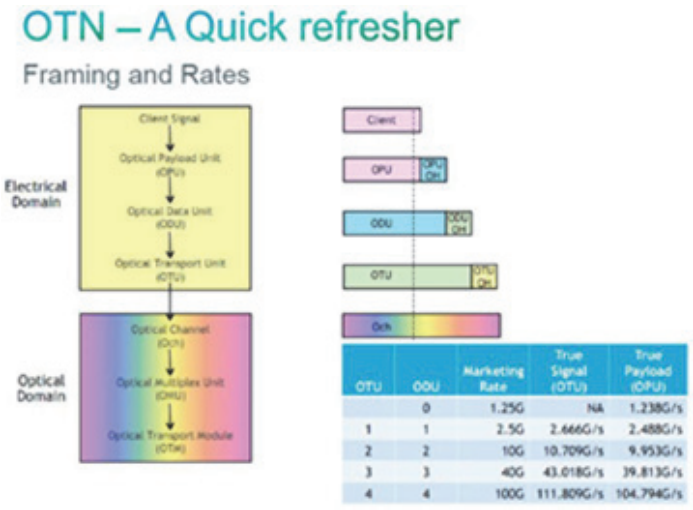


FIGURE 28. ITU-T, Spectral grids for WDM applications: DWDM frequency grid.

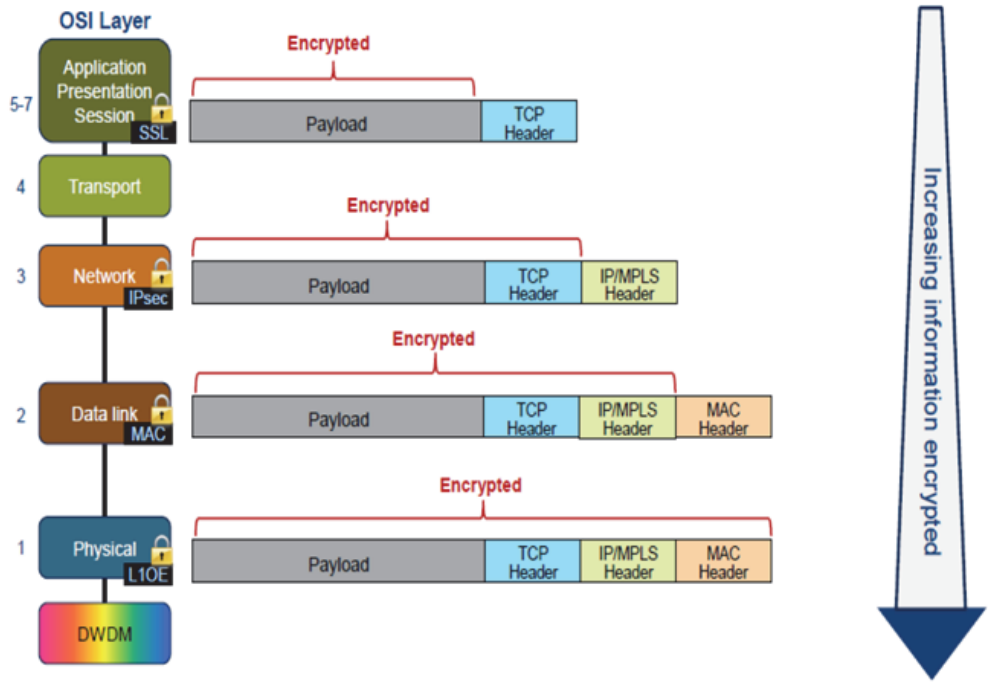


FIGURE 29. OTN, OSI layer and encryption.

3.7.3 Fault location, ITU-T recommendation, G.977/2015

A cable-break point is usually located in an out-of-service condition. Generally, an OTDR is employed for this purpose; a COTDR is used especially in a long distance Optical Fiber Amplifier (OFA) system fault location because of its higher sensitivity and higher frequency selectivity. If optical isolators are used within each OFA, the back-scattered optical pulse, which is indispensable for OTDR measurement, is blocked. One solution for solving this problem is the use of a return path (COTDR path) that should not disturb the in-service traffic as shown in Figures 30 - 32. The transmission penalty

induced by the COTDR path should be taken into account in the power budget. By using such a solution, COTDR facilities may be implemented in OFA systems to monitor the fibre span status. Moreover, if COTDR is employed in an in-service condition in the OFA systems via a return path, this method will have the potential to monitor the gain status of each OFA.

Two different methods may be chosen to implement a COTDR path inside a repeater:

- The first consists of connecting both outputs of one amplifier pair through optical couplers (refer to Figure 30).
- The second consists of connecting the output of one OA to the input of the OA located in the reverse direction (refer to Figures 31 and 32).
- Both solutions allow a bidirectional monitoring.

The definitions and parameters for OTDR and COTDR and related test methods are described in ITU-T G.976.

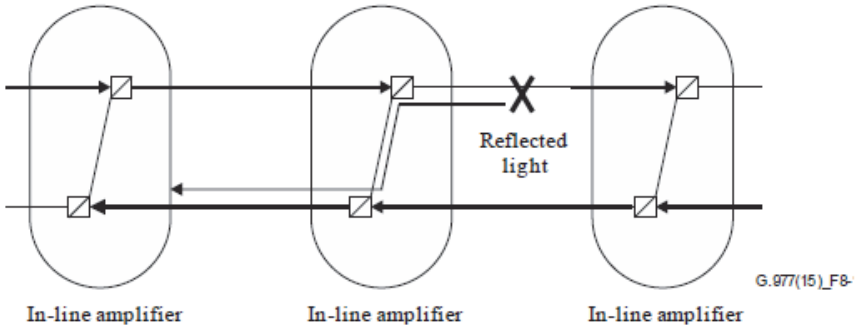


FIGURE 30. Example of a fault location using COTDR for OFA with an output-to-output loopback coupling (ITU-T, G.977).

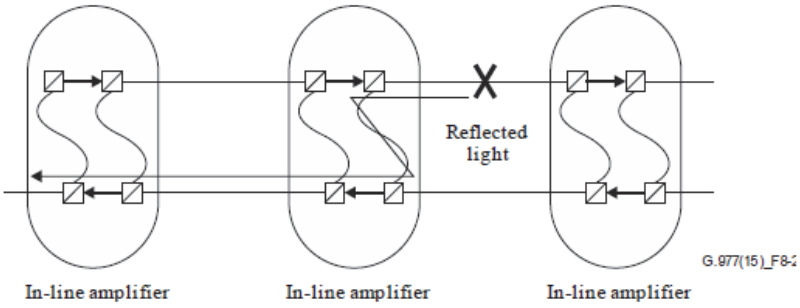


FIGURE 31. Example of a fault location in the first fibre using COTDR for OFA systems using an output-to-input coupler.

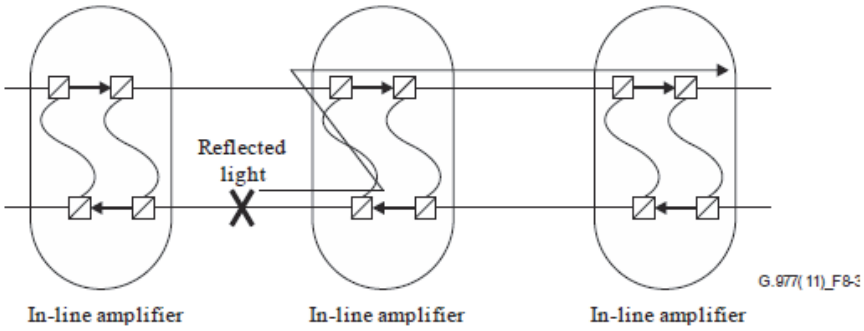


FIGURE 32. Example of a fault location in the second fibre using COTDR for OFA systems using an output-to-input coupler.

We can find more information from reference technologies about the mitigation of transmission impairments in ultra-long band submarine networks (Chesnoy Jose, 2016).

From Table 9, we can see the upper level conceptual submarine cable segment threat matrix, which needs to be taken account when designing and developing undersea submarine optical cable systems.

TABLE 10. Upper Level Conceptual Threat Matrix for Submarine Cable Segment (PII, PIII, PV).

SUBMARINE CABLE SEGMENT THREAT	LAND AND BEACH AREA (Seg. 1)	NEAR SHORE AREA ~50 M (Seg.2)	OFF SHORE AREA ~ 50 – 100 M (Seg.3)	CONTINENTAL SHELF ~ 100 – 200 M (Seg.¤)	DEEP SEA ~ 200 M + (Seg.5)
NATURAL THREATS					
SHARKS					
EARTHQUAKE					
LANDSLIDE					
VOLCANO					
TSUNAMI					
ICEBERG					
OCEAN CURRENTS					
ACCIDENTAL THREATS					
FISHING					
ANCHOR DRAGGING					
DREDGING					
MALICIOUS AND UNDERSEA WARFARE					
CYBER ATTACKS					
VANDALISM					
ACTIVISTS					
THEFT					
TERRORIST					
STATE-ACTORS					
UNDERSEA WARFARE					

Note. Upper level conceptual threat matrix for submarine cable segment (Threats to Undersea Cable Communications, 2017). Threat impact level is shown as colours: Green = Low; Yellow = Medium; Red = High.

3.8 The making and modelling of a threat analysis

Table 11 illustrates the upper level conceptual threat matrix for submarine cable segments based on threats to submarine cable communications. We should also note that cyber attackers, hackers and terrorists can use AI to search from vulnerabilities in submarine optical cable systems through which they can penetrate the systems and services, giving them the ability to attack data centres on different continents. There are many ways that cyber attackers can get inside submarine optical cable systems and gain access to the management and control systems.

Figure 33 presents a threat probability tree model in the Arctic connect cable system. Table 8 divides the depth of the submarine optical cable system into different segments and those segments are divided further into different types of categories of threats. We can calculate the probability of a threat in every segment based on information obtained from international research reports, from the European Space Agency (ESA), from the Arctic statistics from National Aeronautics and Space Administration (NASA), from sensors and sonars, and from news concerning natural or animal cases, accident or injury cases, and cyber-attacks regarding how many times they occur, in what areas and at what time of year. This threat probability calculation can be done for the full length or just a part of the cable system. For the overall situational picture, we also need information about the status of the power supply station.

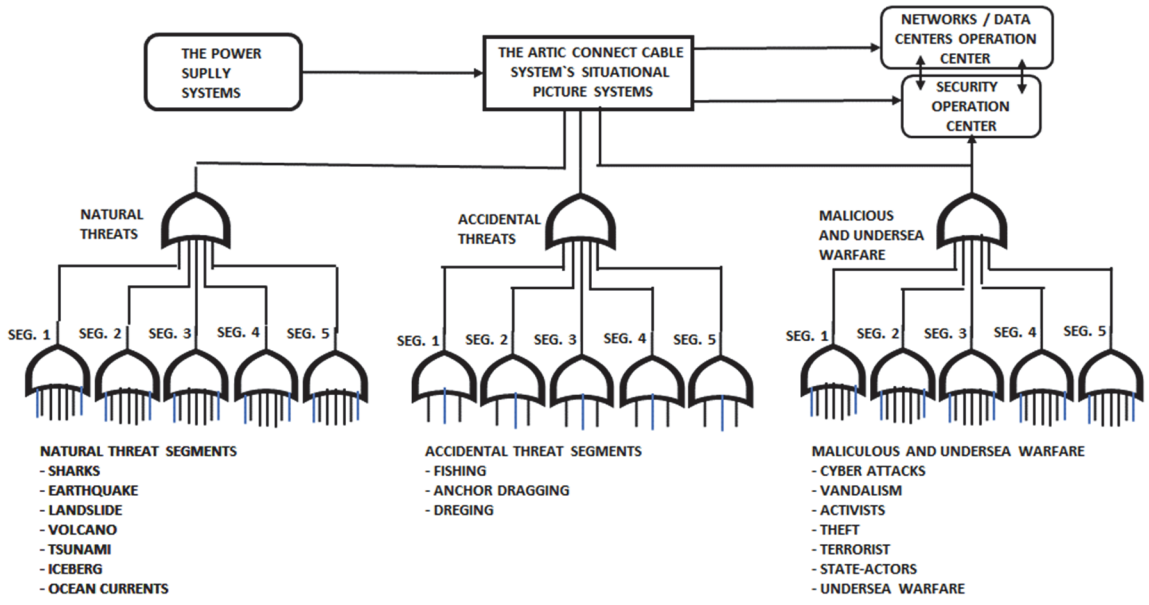


FIGURE 33. An example of the threat tree model for the Arctic cable systems.

TABLE 11. Meaning of Notations

ACTION	EXAMPLES	NOTATION
THREATS OR ATTACK	SUDDEN EVENT, ACCIDENT, TAPPING, EAVESDROPPING, SNIFFING, SCANNING, …,	A
DETECTION	ALARM INFORMATION, SYSTEMS MANAGEMENT INFORMATION, INTERNATIONAL INFORMATION, …,	D
COUNTERMEASURE	ANALYSING OF THREATS AND VULNERABILITIES AND TO REPAIRING, SAFEGUARDS PUT IN PLACE, …,	M

Threats (P(t)), probabilistic threats or attacks happen

$$P1_{S1\ldots7}(t) = P1_{A1\ldots7}(t)(1 - p1_{D1\ldots7}(t))(1 - p1_{M1\ldots7}(t)), \quad (1)$$

to seven different types of natural threats;

$$P2_{S1\ldots3}(t) = P2_{A1\ldots3}(t)(1 - p2_{D1\ldots3}(t)\,(1 - p2_{M1\ldots7}(t)), \quad (2)$$

to three different types of accidental threats; and

$$P3_{S1\ldots7}(t) = P3_{A1\ldots7}(t)(1 - p3_{D1\ldots7}(t))\,(1 - p3_{M1\ldots7}(t)), \quad (3)$$

to seven different types of malicious and undersea warfare.

$$P1_{S1\ldots7}(t) = [(P1_{S1}(t)) + (P1_{s2}(t)) + \ldots + (P1_{s7}(t))], \quad (4)$$

information for the situational picture systems.

$$P2_{S1\ldots3}(t) = [(P2_{S1}(t)) + (P2_{s2}(t)) + (P2_{s3}(t))], \quad (5)$$

information for the situational picture systems.

$$P3_{S1\ldots7}(t) = [(P3_{S1}(t)) + (P3_{s2}(t)) + \ldots + (P3_{s7}(t))], \quad (6)$$

information for the situational picture systems.

Figure 33 shows the situational picture system for every threat-type own threat icon, which shows the situation in each segment of the Arctic connect cable system. Information from the situational system is also sent to the security operation centre (SOC), the network management centres and the data centre management systems. Situational picture systems should be located in different parts of the Arctic connect cable system for network operators and for the service provider because the response time must be fast enough to start, for example, rescue operations. Situational picture information for the whole Arctic connect cable system must also be accessible from the cable operator's operation centre.

The land and beach areas of the submarine optical cables systems are the easiest for attackers to penetrate. When using large capacity systems in undersea environments and new types of modulation technology in those systems, the best possible cable tapping points for cyber attackers are after every OA in deep underwater areas. This offers the attackers various opportunities to obtain a large amount of information from different companies, organisations and governments. In this situation, cyber-attackers and hackers can obtain IP addresses from these companies, organisations and governments and make DDoS, ransomware or malware attacks. Ransomware attacks are typically carried out using a Trojan, entering a system through, for example, a vulnerability in a network service. One possible cyber-attack model is an advanced persistent threat (APT), which is a targeted cyberattack in which an intruder gains access to a network and remains there undetected for a long time. APT attacks typically target organisations such as the national defence, manufacturing and the financial industry, and companies that deal with high-value information, military plans and other data from governments and enterprise organisations. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organisation.

Figures 28 and 29 illustrated that if attackers gain access to the submarine optical cable system that has no encryption system in use, they will also have access to the management system and thus have the ability to do whatever they want for their purpose. The power supply system also needs to be checked for vulnerabilities.

Future communications networks between and within different smart cities present many challenges in terms of the operating environment and heterogeneous telecommunication networks, which contain new devices and systems that are seamlessly interconnected. These new smart devices, IoT – and sensor systems have expanded into homes, office buildings, building automation systems, cars and various control and energy systems, and people are now using their personal smart devices everywhere. These smart city systems also need specific applications, and their information is stored in data centres, as shown in Figures 22 and 23. Hackers, terrorists and cyber attackers thus have many opportunities to find vulnerabilities in this environment and to attack the applications and services of smart cities. Because the data centres are interconnected, hackers and cyber attackers will also be able to attack services and service systems on other continents.

3.9 Answer to the research question, conclusions and future work

Answers to the research questions:

RQ 2: Submarine optical cable systems can be attacked in many ways, including tapping and side channel attacks because it is easy to find the locations of where cables come onto the coast and to thus find cable stations on the beach. It is also easy for terrorists, state actors, activists or other people who want harm the system to attack these stations. Underwater attackers are likely to be mainly state actors because accessing underwater cables requires special capabilities that only state level actors have.

RQ 2.1: From Figures 28 and 29, we can see that if attackers tap the submarine optical cable systems, they will be able to access all information contained inside the optical fibre and use it however they want. The best solution is to use end-to-end encryption in level 2 in Figure 29.

Conclusion

The system to be built is technically very complicated and will need many new technical solutions to meet the required transmission rates and usability and quality parameters. This places considerable demand on the management and control of the system and on the organisation of its maintenance. The changes in social structures will take place very quickly and will affect the implementation and operating models and structures, as well as people's everyday lives and working environments. The current powerful digitalisation trend increases the range of services offered and facilitates their easier use. These developments also have a strong impact on the service chains of the provided services, including subcontractors and their subcontracting chains, hardware solutions, service providers and operating models for every part of the service chain on every continent.

Currently, and in the future, modern communications systems connect data centres and data networks on different continents, enabling real-time communication throughout the world. This type of communication is made possible by undersea optical cable systems, which we use for daily communications. Because submarine cables systems have had such a large strategic impact on our society, they are also a target for hackers, cyber attackers, terrorists and state actors who seek to gain access to the information being transferred across the cable networks between continents. We therefore need to be aware that if cyber attackers can connect to the optical fibres, they could change the ROADM routes, which can lead to the disruption of communication traffic between continents. When considering cyber security in the systems design, we must take into account the upcoming technologies because changes in the cable technology due to dispersion phenomena make it difficult to detect intrusions into the cable system.

Because this new submarine optical cable system (Figure 21) is so long and it is impossible to detect or identify all of the potential attacks, author recommend that an end-to-end encryption system be put in place on each wavelength individually at the lowest layer. Figure 29 illustrates why this is advisable, as we can see the optical traffic network, the OSI layer and the effect this encryption layer has and best solution is the lowest layer encryptions. When we implemented encryption on the lowest layer, we protect our entire communications systems against various types of attacks. Encryption systems of this type are currently in use, but the capacity in which they need to be used may present challenges to using the current systems. The quantum encryption system is currently in operational use; however, such an environment presents challenges to the renewal of encryption keys in each OA. Individual smart devices are also being tested with different types of VPN encryption concepts, and it is hoped that the results will be ready by next year.

Future work

Because the Arctic connect cable system is a critical system that will be used by many countries, organisations and individuals, it is essential to examine the key issues affecting its functioning [59].

- With regard to cyber security, the use of AI and its potential to protect submarine optical cable systems needs to be investigated to better protect against malware and cyber-attacks.
- The possible use of COTDR should be investigated because it is used for searching for faults and can also be used to detect the tapping of cable connections.
- We must investigate a variety of protection mechanisms for submarine optical cables systems because it is an extremely important fibre optic connection between different continents.
- The effect of different encryption systems, such as quantum encryption or Layer 1 - 2 encryption systems, should also be tested.

CHAPTER 4. THREAT CHARACTERISATION FOR VARIOUS LAYERS OF INFRASTRUCTURE

This chapter is based on the author's research on threat characterisation for various layers of infrastructure in the Arctic region (PIII) and incorporates the materials and working group discussions for the paper presented at the Governance for Cyber Security and Resilience in the Arctic, 2019 NATO conference held in Rovaniemi, Finland. In Rovaniemi, the author presented the future smart cities and smart societies based on Figures 4 - 6 in Chapter 2 and Figures 20 - 23 in Chapter 3 of this dissertation. Figures 43 - 45 are based on those Figures 4 - 6 but there are differences in the Arctic region services, which are written in red in Chapter 4. There are materials of PII, PIII and PV.

4.1 Introduction

To identify and define threats and perform a threats analysis for various layers of the infrastructure, we must first look at the Arctic region as a whole as well as its component structures including where people live, how they move, what type of buildings are used in the region and where the cities are located. We also need to look at the natural resources in terms of which region they are in, which companies are working there and what services they need for their everyday functions.

The Arctic region is often defined as the area where the average temperature for the warmest month is below 10°C. Figure 34 shows the Arctic region as defined by this criteria, comprising the area inside the red line. The Arctic region's inhospitable weather and other environmental challenges have limited human activity and settlement to below 78° north latitude (ARCTIC CIRCLE). The Arctic region is one of the least populated areas in the world and there are only a few large cities. About half of the Arctic population lives in Russia. The three most numerous population centres above the Arctic Circle lie in Russia: Murmansk (population around 300,000), Norilsk (over 170,000) and Vorkuta (around 60,000). Tromsø, Norway has about 71,000 inhabitants, and Reykjavík, Iceland has more than 100,000.

Most of the roughly four million inhabitants live on lands bordering the Arctic Ocean. The population is a mix of Caucasians and several major groups of indigenous peoples, who have lived in the north polar lands for centuries. Caucasians make up sizable portions of Siberia's and Greenland's populations, and a near-majority in Iceland. However, there are also representatives of many different groups in the region such as the Inuit, Chukchi, Sami, Yupik and Inupiat people. Typically, the people who live in the far north are nomadic hunter/gatherers with the emphasis on hunting rather than gathering, though the Sami people of Scandinavia amongst others are reindeer herders. During the 20th century, immigrants came to the Arctic region for job opportunities. For the most part, they did work relating to the natural resources in the region. This large influx of immigrants dramatically changed the balance of non-indigenous and indigenous people in many areas.

FIGURE 34. The Arctic region.

This migration has affected the infrastructure, towns and villages throughout whole of the Arctic region, including the available services and the ecosystem. Companies in the region already take advantage of the oil and gas resources. The employees of these companies require a variety of services, such as health care, children's schools, banking services and leisure facilities. While the growing tourism in the regions requires its own services, better services must also be offered to indigenous peoples in relation to health care, children's school and the services provided by shops.

The Arctic region contains a large part of the world's multi-year sea ice, which is 3-4 m thick on average with many even thicker ridges. Greenland holds the largest glacier in the Arctic. When a piece of the Greenland glacier breaks off, it forms an iceberg. Most of the iceberg is located underwater, but since the ice is not quite as dense as the water, about one ninth of it remains above the surface. Figure 35 shows the Arctic Ocean and the bordering countries with summer sea ice cover. The Arctic region has some of the most extreme climatic conditions on Earth. Average winter temperatures vary from -40 to 0°C and there are areas where temperatures often fall below -50°C. These temperatures mean that all structures above the ground are covered in the winter by thick ice and by snow blown in by the wind. Strong storm winds contribute to the difficulty of planning and building permanent infrastructures in the area. The decline of ice cover during the summer allows for only a few weeks of work without the help of icebreakers.

FIGURE 35. The Arctic Ocean with the summer sea ice cover (Arctic Ocean Map).

There are also geologically active areas below sea level in the Arctic, which can limit the various forms of construction and development in the region. Geologists have found that there are even underwater volcanoes melting the Arctic Ice (Robert, 2016). The Gakkel Ridge is a gigantic chain of underwater volcanoes snaking 1,800 kilometres beneath the Arctic Ocean from the northern tip of Greenland to Siberia (Figure 36).

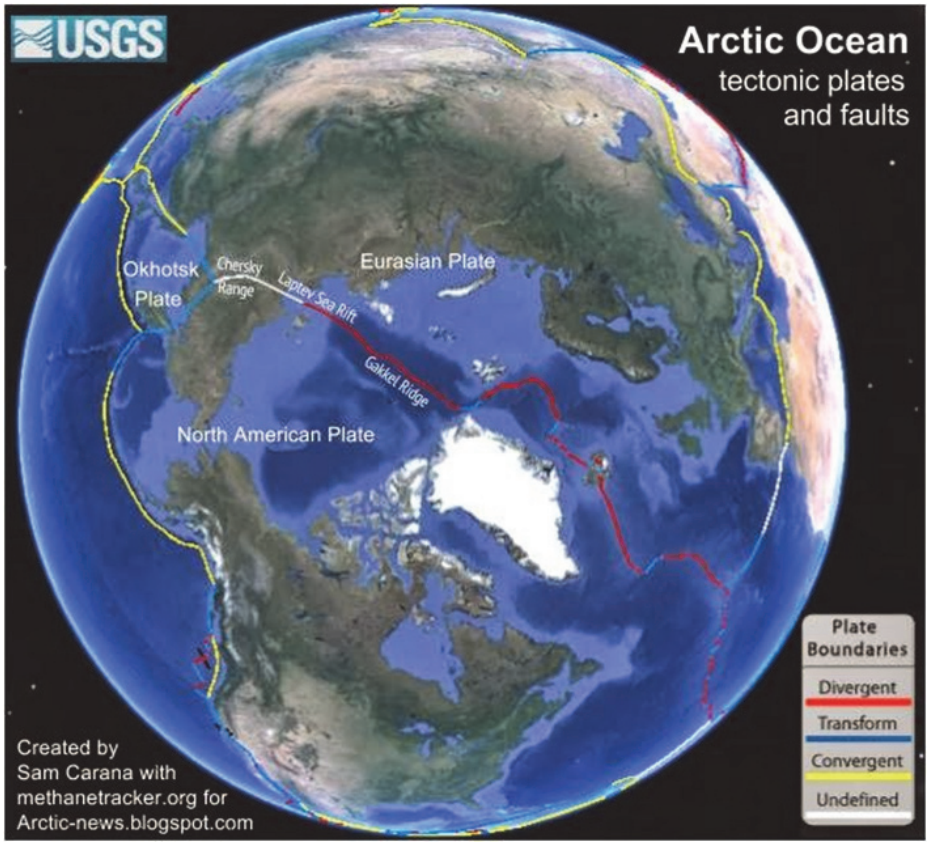


FIGURE 36. The area of the Arctic region's undersea volcanoes and tectonic plates (Robert, 2016).

When designing infrastructures for the Arctic region, we need to take into consideration these underwater volcanoes and how they might impact our planned construction (Figure 36).

Powerful geological heat flow forces deep in the Arctic Ocean are melting the ice. These underwater volcanoes may also erupt at some point in the future and cause considerable damage to the Arctic region and its infrastructures (Kent, 2015). However, the Arctic region also contains a large amount of natural resources, especially oil and gas (Figure 37), which are of interest to several states (Hobart, King, 2016). The exploitation of those resources under these conditions is a challenge because of cold weather and it is necessary to take these extreme conditions into account in all situations.

FIGURE 37. Oil and natural gas resources of the Arctic.

The Arctic Oil and Natural Gas Provinces Map is seen in Figure 38. The United States Geological Survey estimates that over 87% of the Arctic's oil and natural gas resource (about 360 billion barrels oil equivalent) is located in seven Arctic basin provinces: the Amerasian Basin, Arctic Alaska Basin, East Barents Basin, East Greenland Rift Basin, West Greenland-East Canada Basin, West Siberian Basin and the Yenisey-Khatanga Basin. The Arctic region is shared between different countries, as shown in Figure 38 (Hobart , King).

FIGURE 38. The division of the Arctic region between different countries.

The countries shown in Figure 38 exploit the natural resources in their respective areas (Figures 37 and 38), which means that they are also developing the infrastructures, communications and necessary services for those areas. When we consider the situation presented in Figures 34 - 38, we can see that the Arctic region has many opportunities for cooperation and many requirements for the people living there. To take account of people's service needs and to assess the needs of the communications systems for the different parts of the Arctic region, we must also look at where people actually live in the Arctic region. The indigenous peoples who have lived in the Arctic region for centuries and the newer immigrants all live in areas that best suit their needs (Figure 39).

FIGURE 39. Population centres in the north.

Figure 39 also shows that people live in quite scattered areas throughout the Arctic region (THE ARCTIC, population) (Population centers in the north). Only in the regions of northern Europe and the European side of Russia can larger numbers of people and cities be found. Challenges related to mobility hamper the lives of people living in the Arctic regions (Figure 40). The use of onboard navigating, especially in the winter, is very challenging if there are no transport systems that are suitable for use under these conditions.

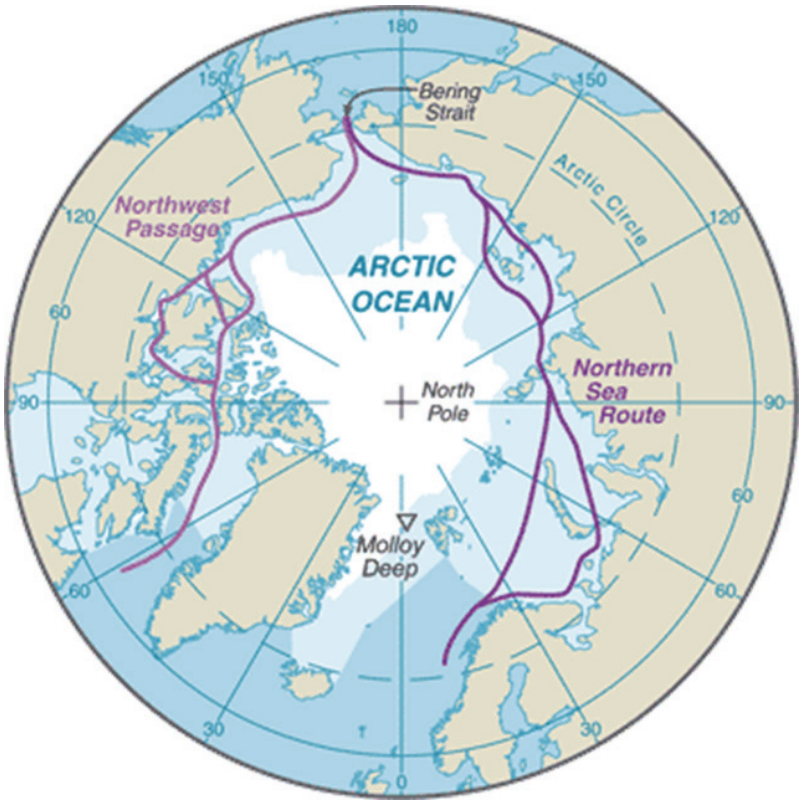


FIGURE 40. Polar regions map with the Arctic Ocean sea routes (Geology.com).

Future infrastructures and, information and communication systems need to be designed and adapted to work in these challenging environments. A large communication capacity and many new contact points will be needed in the future to satisfy the data transfer needs of users, businesses organisations and governments in these areas. These areas require proper and reliable communication connections so that they can communicate and use the services offered by the rest of the world. The regional development and joint operations of these northern areas also require reliable communication connections such as those provided submarine optical communications systems and satellite systems. These new connections provide people in the area with real-time access to existing digital services in their home country as well as the ability to communicate with their friends locally or elsewhere in the world.

A good service option is satellite communications, which allow for the flexibility of services required in the Arctic. However, there are some challenges to implementing satellite communications in the Arctic region. One of these challenges is coverage. The two main regions to be covered are the Polar area above 75°N and the area between 66°N and 75°N. These areas are outside the geostationary coverage area of the Arctic. These areas are further divided into a European part, a Russian part and a part of North America. The main challenge related to future satellite communications in the Arctic is securing broadband access, where the coverage of geostationary satellites is lacking. In certain situations, it is possible to obtain better coverage area in a particular area by using High Altitude Platform Services (HAPS) system (Hummelholm, S-72.4210, 31.1.2006).

When developing future infrastructures and information and communication systems in the Arctic regions, there is also a need to examine use cases, from which we can define the requirements for infrastructures, services and information and communications. Use cases from oil and gas companies and mining companies are useful for the development of the Arctic regions because, based on the use cases, we can identify the dependencies and risks from the requirements of the system. When we have the use cases, we can define the different types of architectures required for each service. These architectures include infrastructure architectures, integrations architectures, security and cybersecurity architectures and smart device architectures. Once we have determined the defined risks to these systems, we can conduct a risk analysis, identify the vulnerabilities of our current systems and services, define the threats and cyber threats and perform a threats analysis.

In the development of future infrastructures in the Arctic region, we must take care to follow EU directives and guidelines as well as international agreements and laws. This information guides designers and developers in the right direction for developments. Because the Arctic regions cover a large area that is difficult to build in, the question of expense is raised in terms of what is reasonable and what is not.

4.2 Objective and grouping of the chapter

The research question of this chapter asks whether it is possible to develop reliable submarine optical cable and satellite systems for communications between the various Arctic regions to provide citizens there with the necessary and reliable services.

This study defines functional segments that can be used as a guide when outlining the infrastructures, services and architectures that are needed to form the Arctic region's ecosystem. The architectural descriptions can be as accurate as needed, depending on the service needs of the region and the specific requirements of the service. Different architectures are also needed to develop the services and to assess the cyber threats. Once the Arctic's ecosystem architectures are defined, the dependencies, risks, vulnerabilities and cyber threats can then be explored. This research will also look for dependencies on various activities and services that can be used to identify risks and to carry out risk analyses. In addition, there are several vulnerabilities in various functions and service systems in the Arctic region from which we can further identify risks and examine cyber threats. This study also seeks to define a model to facilitate threat assessments and the comparison of threats and to facilitate the analysis of threats in the Arctic region's ecosystem. Regarding the technical design criteria, we also need to take into account different type of threats such as natural threats, accidents, terrorists and cyber-attacks. The results obtained through the model aim to facilitate the design and implementation of architectural solutions. The implemented model can help to better assess the likelihood of future attacks on the Arctic infrastructures, submarine optical cable systems, satellite systems, and threats to future services in this region. Chapter 4.3 present the research questions.

Chapter 4.4 present the ecosystems and future operating environments of the Arctic region, the submarine optical cables communications networks, mobile networks, satellite networks, HAPS [68] networks and data centres at a general level.

Technical solutions are also provided to address climate questions and opportunities to reduce energy consumptions in these new technical solutions for the Arctic region. Chapter 4.5 present new renewable energy systems to the Arctic region and chapter 4.6 present background information used in this Arctic region chapter. Chapter 4.7 present technologies in the Arctic region in the future.

Chapter 4.8 present natural threats, accidental threats and cyber threats in the Arctic region and chapter 4.9 describe the threats associated with the submarine optical cable systems in the Arctic region. In chapter 4.10 is given presentation of making and modelling of a threat analysis. In chapter 4.11 is given answer to the research questions, made conclusions and given information from future research work.

4.3 The research questions addressed in Chapter 4 are as follows

RQ 3. How can we provide services to the citizens of the Arctic region?

> RQ 3.1. How can we implement a new type of energy efficient building, which also reduces CO_2 and greenhouse gas emissions in the Arctic region?
>
> RQ 3.2. How can we implement new types of smart city and building architectures so that we can eliminate CO_2 and other greenhouse gases and save city space?

4.4 Description of the future operating environment and technology

The Arctic region's inhospitable weather and other environmental challenges have led to limited human activity and settlement in the area (Figures 34 – 39). This cold environment also poses challenges in terms of providing services, exampled communications services and healthcare services, to the people living in the Arctic.

Figure 39 shows the current population centres in the different regions. The existing and planned Arctic submarine optical cable systems now and in the near future are based on where the cities of the Arctic region are located and where people are living, as shown in Figures 39 and 41.

Communications possibilities are coming better, because Cinia is planning to install a submarine optical cable between Kirkenes, Anadyr, Japan and China because those regions need good communications systems now and in the future. Cinia provides secure high availability networking and software solutions to the customers in those areas.

Author was involved in meeting at the NATO workshop in Rovaniemi on 27-30 January 2019, where discussed of Governance for Cyber Security and Resilience in the Arctic.

Main discussion areas in that meeting was - "Defense, transportation, and business opportunities in the Arctic are accompanied by the danger of cyber-threats, especially to critical infrastructures which in the Arctic become "extra critical" because of the harsh environmental climatic conditions and remoteness. Critical infrastructure in the Arctic is also crucial for military and security since it hosts many data hubs, significant energy

resources, and digitized infrastructural assets dependent upon secure and reliable computer control. Interferences with climatic conditions, ice, and disasters requires new methodologies of risk and resilience assessment but also effective legal frameworks able to protect critical infrastructures and sustain both industrial and military activities".

FIGURE 41. The Arctic region undersea optical cable systems now and in the near future (PII, PIII and PV).

Many factors affect the future of the Arctic region and its ecosystem. The political issues of the Arctic region, climate issues and various conflicts of interest between the various groups are some of these factors. Figure 42 presents the rapid change factors affecting the Arctic structures, the lives of people there, and the culture and environment of the Arctic region. We need to consider these factors of change and their effects on various activities in detail, so that we can accurately plan the structures and service and development needs of the Arctic region's ecosystem.

To provide services to the right place and at the right time over such a large area, it is useful to group the Arctic regions services into the different segments in which the current structures and services can be located. Future Arctic regions structures can be divided into the different service sectors shown in Figure 43: infrastructure, energy, buildings and homes, mobility, telecommunications, public and private services. Each set of operations has its own service and communication needs depending on the user group. Such groups include the indigenous peoples, immigrants, peoples living in a

particular area, design and maintenance personnel, financial staff, telecom and service operator's staff, virtual service providers and operators, state actors and administrative actors.

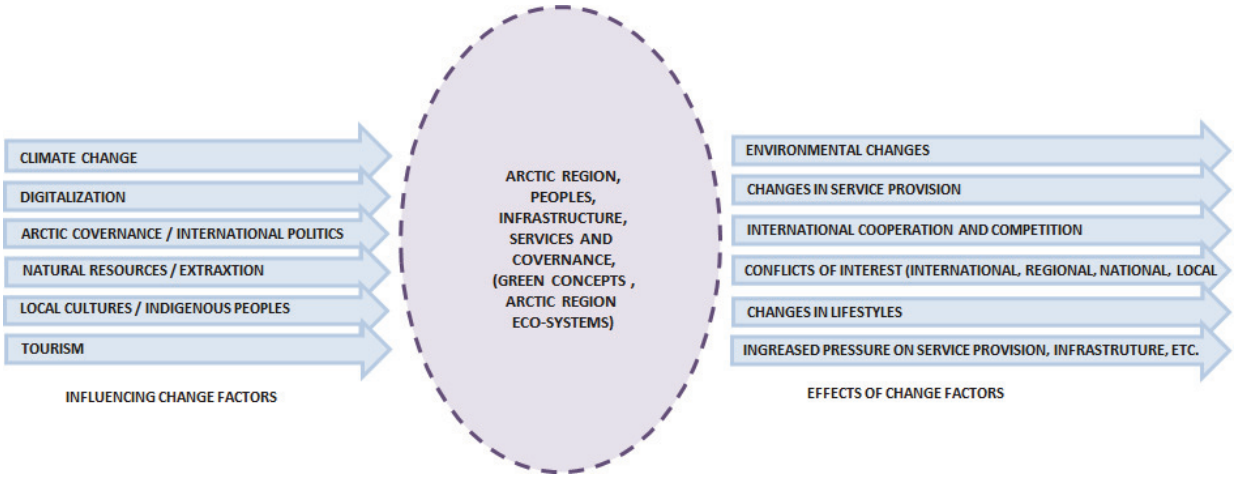


FIGURE 42. Variables affecting the future Arctic society (PIII, PV).

Figure 43 is an example of the way the segments can be grouped depending on the situation and region. The description is not exhaustive, but the more accurate grouping of factors we achieve, the better we can take into account the specific needs of different use cases and identify the needs of various people, businesses and regions, as well as the co-operation needs of different states and different interest groups. Each group of users operates horizontally in their service sector, as shown in Figure 44. Figures 43 - 45 seem to be more similar than Figures 4 - 6, but there are differences within the Figures relating to the services (marked in red). Special services in the Arctic region were taken into account (Figures 43 - 45). The author discussed the services needed in the Arctic region with researchers from the University of Rovaniemi and they are analysed these needed services there in different regions in the Arctic.

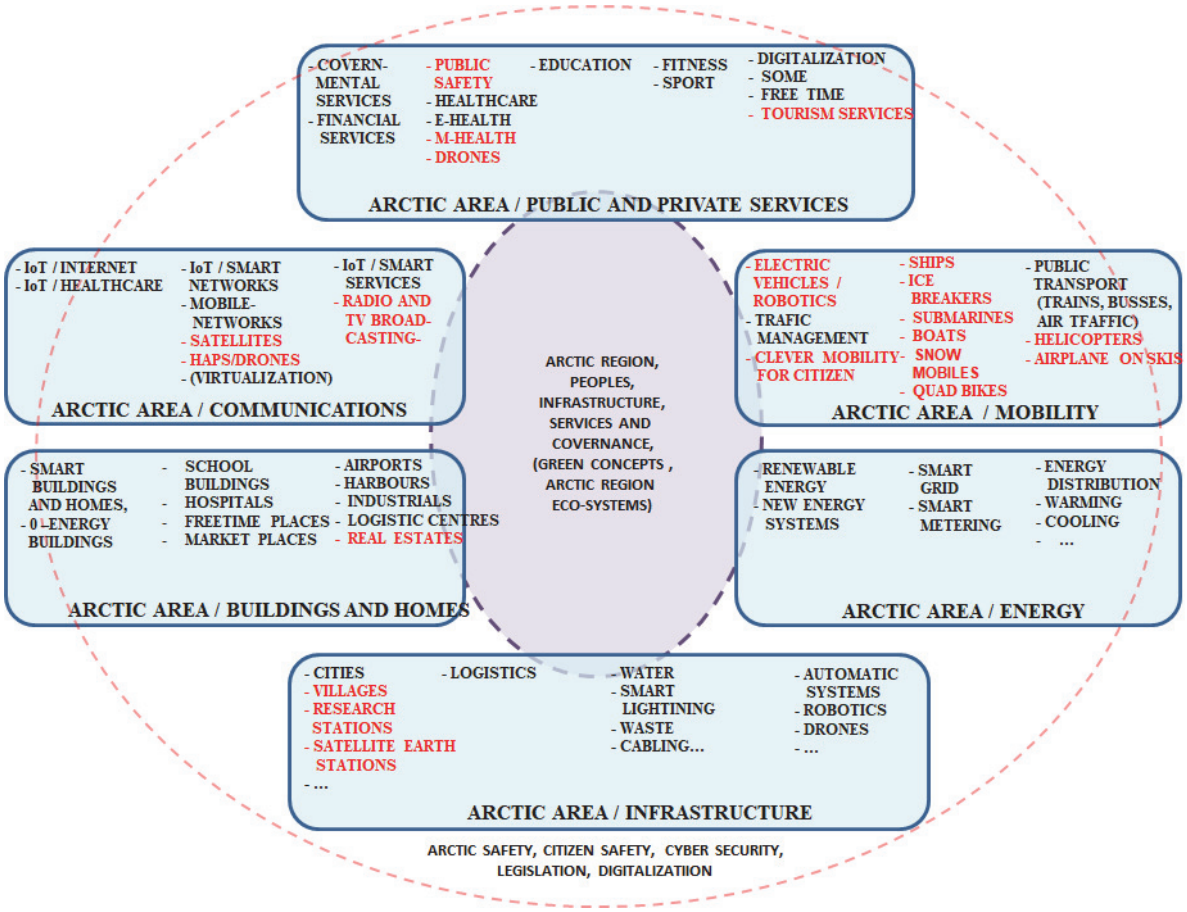


FIGURE 43. Functional segments in the Arctic region (PIII, PV).

For the Arctic regions to function properly as a whole and provide the citizens with the necessary digital services, the information systems in the various service sectors need to be able to work together and exchange information vertically so that the services of the Arctic regions can be implemented flexibly and efficiently. The information systems used by different service sectors or the smaller entities within them, however, are often in different phases of their life cycle. In the future, the Arctic region could be seen as one entity in which co-operative efforts between different countries and user groups should be made possible due to a difficult and sometimes critical living environment. This means that everyone should have access to the same services and be able to use them in a critical situation, example in a rescue situation, or to obtain information in some way from other countries to obtain assistance in certain situations like ship accidents. This in turn means that we need both horizontal and vertical communications opportunities between different user groups and that we must perform cyber analyses horizontally and vertically on those infrastructures, communications systems and services. Consequently, the integration between information systems may not succeed because data models, operating systems, management systems and application interfaces may not work well together. Their coordination and the success of the data exchange through integration environments are very challenging (one author remarks: a lot of cooperation is needed between different operators and countries). The system platform solutions in place can also be different, delivered by different vendors and may have their own de facto standards

that are incompatible with the equipment and systems from other equipment vendors. This may result in the use of certain types of platform solutions to guarantee the functionality of some particular system until renewal is worthwhile or until it becomes timely with the end of its lifecycle.

The security solutions for systems and services may also be different and even partially incomplete leading to practical challenges: for example, it may be impossible to combine the various systems (make federations) and to thus make different services compatible. Each entity may also contain information at different security levels, which must be properly protected and controlled. To develop the Arctic region infrastructure, services and management in the future while taking care to remember green concept in the Arctic region, we must be sure to check the international laws and regulations, EU directives and regulations, national laws and regulations, use cases, requirements, dependencies (Figure 44). As a result of the ongoing developments in the Arctic region, people will produce huge amounts of information in the future that will need to be processed and stored. Additionally, services based on technically outdated solutions will be used alongside new technology. Therefore, future information and communication systems must be designed and adapted to work together in this challenging business environment where security threats and cyber threats are present everywhere.

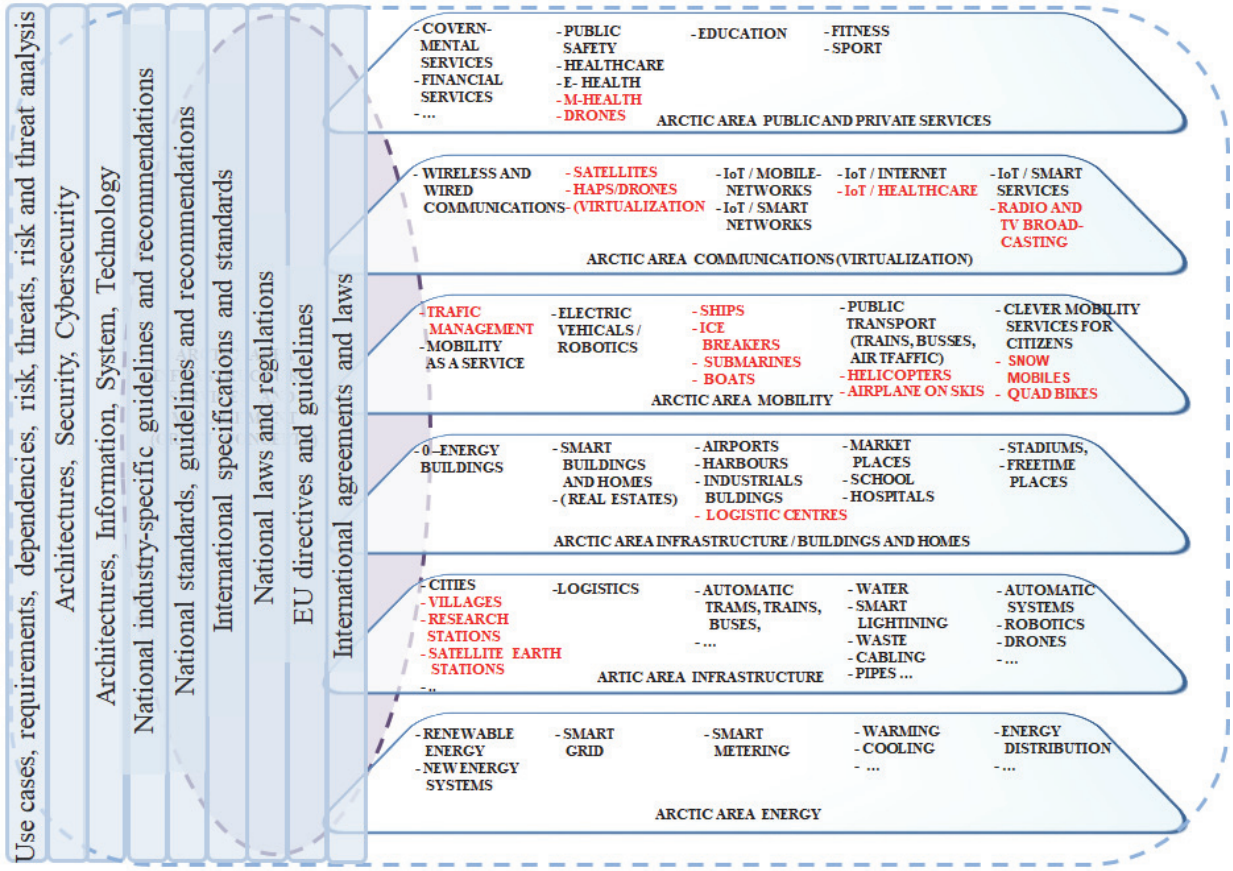


FIGURE 44. Functional segments in the Arctic region (PIII, PV).

When dealing with technology and segments in the Arctic, we divide the geographical area into three parts: the mainland, the sea and the coastal areas. The

mainland includes smart cities and the connections between them, while the coastal and marine areas involves the submarine optical cable systems, coastal landing stations and data centres.

Before we start to design or develop the Arctic regions infrastructure and services, we must also review the variables affecting the future of the Arctic society, as seen in Figure 45. Figure 45 is divided into three parts: (1) the most rapidly changing situations, (2) the Arctic region and (3) digital information in the Arctic region for politicians and policymakers, who make decisions based on digital knowledge, and provide laws and guidelines to develop the Arctic region (Figure 45).

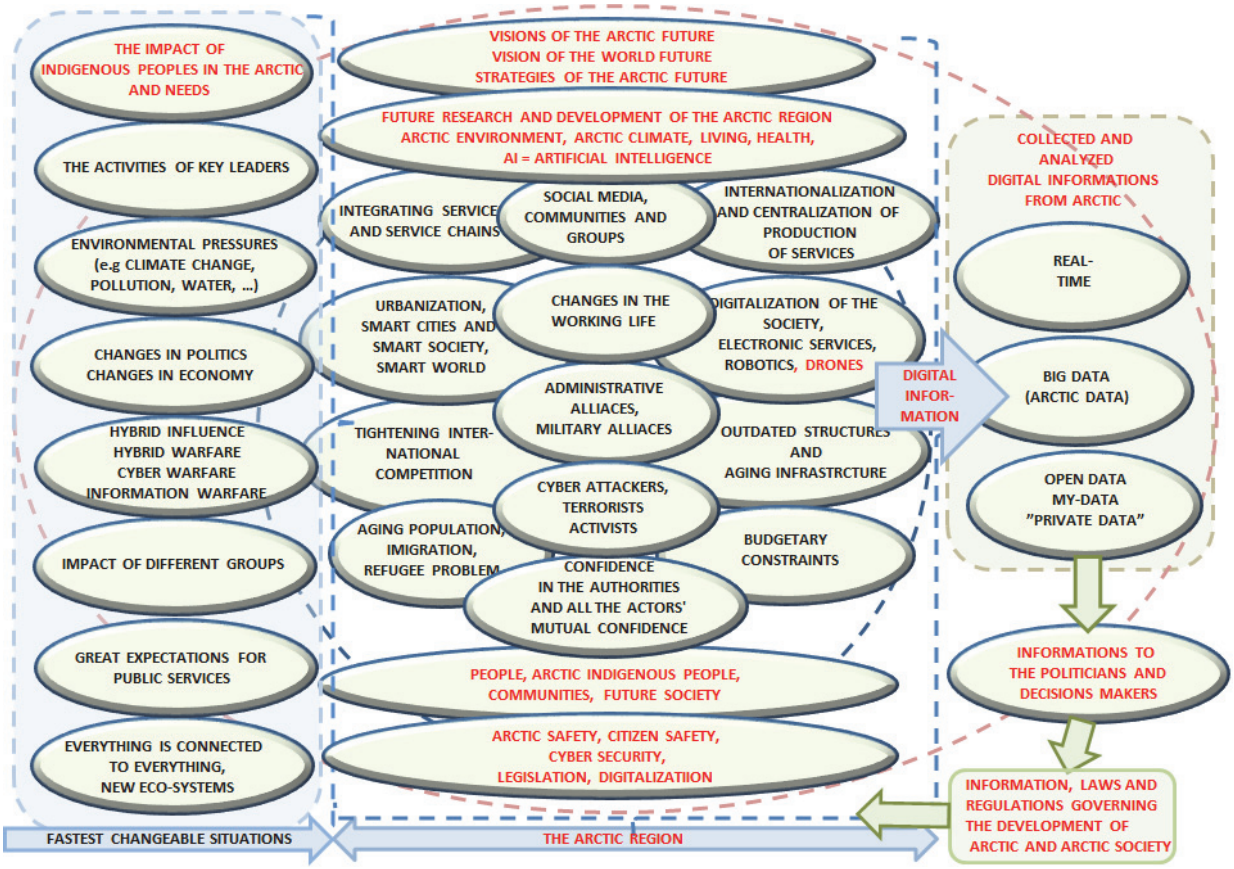


FIGURE 45. Variables affecting the future of Arctic society (PIII, PV).

Figure 45 shows that many different types of functions need to be managed and many different types of groups exist, including political or local groups or the indigenous peoples, immigrants and peoples living in the area. All those functions drive changes in the Arctic region to a greater or lesser degree and provide their ideas to the Arctic region's developments and deciding in which directions it must be developed.

4.4.1 The Arctic region and energy

The most important segment in the society is energy (Figure 44). All forms of functionality in the Arctic region and in any smart society and smart city depend heavily

on a supply of electricity. While it is possible that a smart grid and heating, cooling and energy distribution systems may collapse due to internal faults, such failures could also be caused by cyber-attacks. Cyber-attacks have also been made against power stations to its managements systems, which means that electricity-based systems in the distribution area of the power station are not working any layer, seen in Figure 44. We use different fuels for homes, cars, ships and planes; however, it is not possible to pump fuel into a fuel tank without electricity in many cases. Many systems use diesel generators to cope with such incidents, but the operation time of backup systems is limited. For communications systems, the emergency power arrangements are only classified by hours (6 or 12 hours), unless spare diesel generators are available. Even if the energy systems are working properly, the geomagnetic storms in the Arctic can cause interferences in long electrical power transmission lines and interfere with or even destroy electrical equipment (Max Power, 2014).

The above descriptions provide some reasons why investigating and developing renewable energy sources has such a strong influence on the Arctic region's systems both now and in the future. Gwen Holdmann, Director of the Alaska Center for Energy and Power, stated,

> "The Arctic as a whole is a real leader in renewable energy development – almost half of the power is produced from renewable resources, well over double the global average. This means also that when you can produce wind power, hydro power, solar power or any kind of renewable energy form of any type of electricity, and if there are not enough local users, you can feed the extra energy to the electricity grid for other users. When there is a small electricity grid where users are much closer, if the extra electricity is generated, someone can use it almost immediately"[2].

It is also not so easy for cyber attackers to attack such renewable energy systems because the systems management is located close to the production facilities, meaning they are fairly easy to manage, they can be used to check the people who work there and when, and there are not needed any connections to the Internet to system work. When renewable energy is plentiful and therefore generates excess energy, it should be possible to store that extra energy, for example, in fuel cell systems and use that fuel cell energy later. The Arctic region has many renewable energy sources including geothermal energy, solar fuel, solar panels and next generation nuclear power systems (Small Nuclear Power Reactor).

4.4.2 The infrastructure of the Arctic region

The Arctic region has cities, villages, research stations and satellite earth stations that need various services, like banking, healthcare and travelling, and those infrastructures must be connected to the communications systems in one way or another. Those infrastructures also need electricity, water systems, smart lighting systems, waste systems and trams, trains, buses, airplanes and ships (Figure 44). One of the largest systems requirements is logistics, which is needed on both the ground and sea portions

[2] Hanna Hoag, 2016.

of the region. There are many different types of services which are available to citizens in this kind of environments that they need in their everyday lives. However, when these communication systems and services are used, it means that there are opportunities for cyber-attackers and hackers to attack those systems and disrupt their use.

4.4.3 The infrastructure of the Arctic region – buildings and homes

Buildings and homes are dealing with energy efficiency issues better than ever before because the Arctic region are used renewable energy systems. People are now talking about zero-energy houses and buildings everywhere, which use the newest energy efficient solutions. However, same time many devices and sensors are coming into the buildings, making buildings infrastructures vulnerable to cyber-attacks. Attackers have already carried out many attacks throughout the world against these types of environments and systems.

Figure 46 shows a future office building and its infrastructure services and communications systems and services. Most IoT devices and sensor systems are connected to the communication's access node in the room using wireless technology through which node information is transmitted to the building's communications access node in the cross-connection room. These buildings contain local area networks (LANs) to which all IoT and sensor devices are connected through either wireless or fixed systems. People who are working inside the buildings use the same connections and systems as the IoT devices and sensors and at the same time. Thus, when we look for possible security issues that might impact these types of systems, there are many security and cyber security issues to consider. This is a question of not only the size of the building, but also of installing new types of IoT devices and sensors in everybody's homes. When people use e-health or m-health systems in their home, there are many opportunities for interference between those devices and the home systems because they use the same frequencies in the same frequency bands. Nowadays, many patients are sent home with various sensors so that healthcare staff can track their conditions. There are many different types of vulnerabilities in those systems, which hackers and cyber-attackers can take advantage of to hack into different systems in the surrounding cities and society. One big future challenge concern zero-energy buildings because mobile communications systems do not work properly when people use their smart devices inside the buildings. Buildings walls attenuations are too high for wireless communications systems to work properly. If we consider the Arctic regions, this situation is even more challenging because the connections are not as good as and a patient's vital information must be seen by the hospital database in real time. The same situational concern also pertains to different types of critical systems like rescue situations in the Arctic region.

Corridors and canals can be built underground for cables, electric supply systems, robotic vehicles, intelligent logistics, water pipes, waste systems and heating pipes as needed. This setup opens up opportunities to develop energy efficient solutions for smart city infrastructures in the Arctic region (Figure 46).

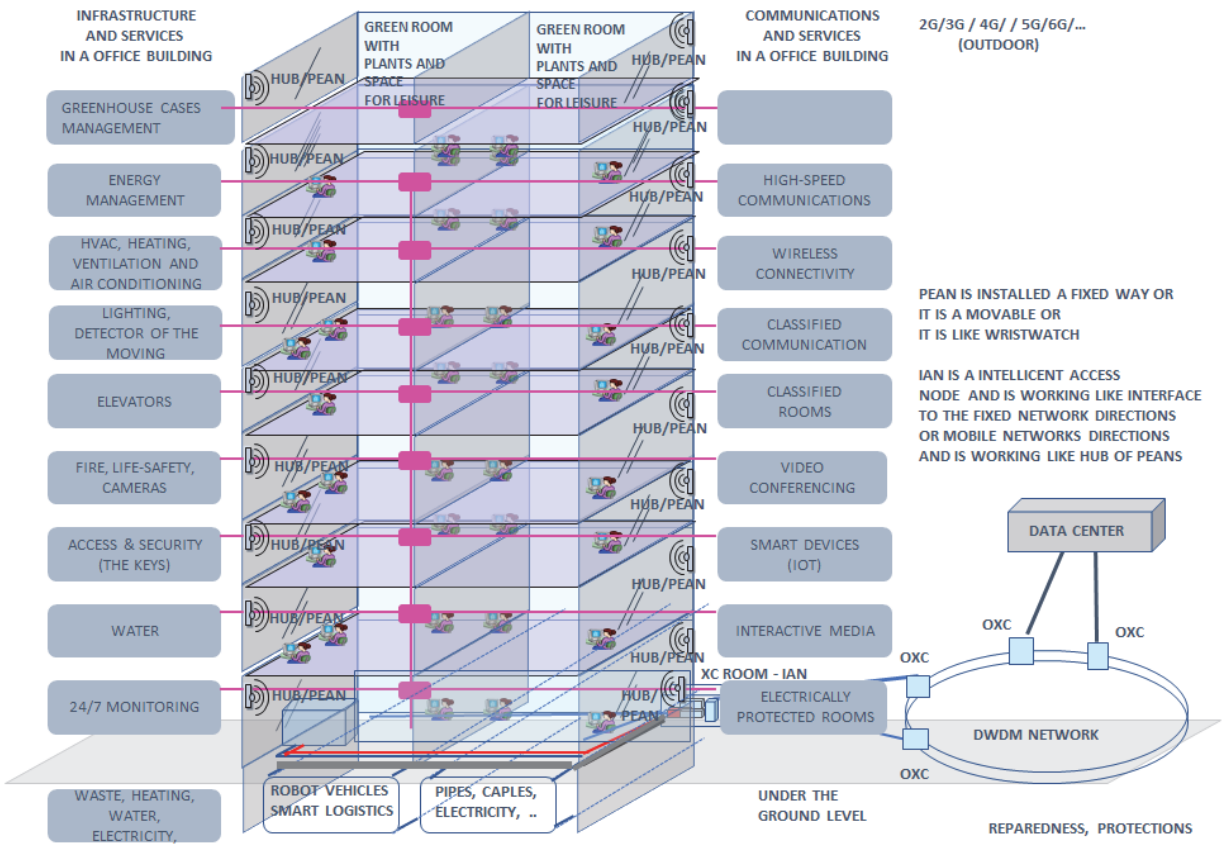


FIGURE 46. A future office building with its infrastructure and communications systems.

Additionally, robot traffic can be used to transport freight to and from the cities and to freight centres, to transport waste to the waste stations and collection points, and to provide better and more reliable transport systems in general. Underground vehicles, such as the METRO, have been used for a long time in many cities; it is possible to expand this system for other purposes like waste transports. In the future, we also need smart lighting, traffic management and intelligent traffic operations to reduce energy consumption and greenhouse gases. By transferring some of the infrastructure to underground, we are also freeing up terrestrial space for the development and construction of the smart city infrastructures, as there is not always enough space in town centres to build and develop future services and facilities. In this way, people can be better provided with the services they need.

Deforestation, especially the destruction of rainforests, is a major societal challenge which is reducing carbon sinks all over the world at a rapid pace. This tree issues must also be taken care of in future cities and societies so that we have enough parks and trees inside the parks in the urban environment. Additionally, with regard to rainforests, since the reduction of greenhouse gases is no longer a local matter, it must be seen as a whole, taking into account the situation in various parts of the planet to reduce greenhouse gases and the carbon footprint as effectively as possible, sufficiently and quickly.

To illustrate this problem, we can watch the air pollution flow across the planet in real time at this address: https://www.sciencemag.org/news/2016/11/watch-air-pollution-flow-across-planet-real-time. Scientist Yann Boquillod founded AirVisual

Earth, which is an online air pollution map based on data from satellites and more than 8,000 monitoring stations to display global air pollution in real time. We can also watch how quickly the rainforest areas are disappearing from the globe (Hansen).

In Eno, located in the North Karelia region of Finland, elementary school teacher Mika Vanhanen founded the Global Sustainability Web School 2000. To date, 10,000 schools in nearly 160 countries have already participated in its activities which focus on environmental issues such as tree planting. The goal was to plant 100,000,000 trees and the target was reached in 2017. In the same year, the organisation received an idea from peoples for an international climate school for school children (Vanhanen).

Figure 46 presented the future office building with infrastructure and communications systems. In the future, smart homes in smart cities are expected to use solar panels, geothermal energy and new types of wind power generators in a hybrid mode. The new types of wind power generators can be installed on the top of buildings (either alone or in a wind generator group) to produce energy for either the building's needs or other local buildings' needs, or even to contribute to the main grid (as used nowadays in Finland). Inside the buildings, there is the possibility of building green rooms with green walls on different floors and building greenhouse gas removal systems to remove greenhouse gases from inside the building (Figure 46). New buildings should be designed in ways that address green values and green energy and reduce greenhouse gases.

The future building described above means that the development of smart cities and smart societies requires a high level of coordination and cooperation so that we can build the required infrastructure and communications and service systems while ensuring safety, security and cybersecurity concerns are addressed in every segment and for every service inside and between the segments (Figures 6 and 44). After addressing those issues in the segments and between the segments, we will be able to look at the Production, Supply, Service, Subcontracting, and Maintenance chains from end-to-end in smart cities and smart societies with sufficient accuracy. It will then be possible to take into account the necessary issues for long-term planning and development, and because all the necessary elements can be seen along with their operating environments, technical solutions and service portfolios may be implemented in accordance with the EA framework (Dragon1-open) (JHS 179) (Figure 7). When we use EA framework, this means that all involved parties will have the exact and real knowledge of development needs and their impact on different segments, the services within segments and inter-segment services, as well as services provided to citizens. These development needs are also particularly important because of the digitalisation of all information and the digital form of services provided on different networks. Because everything is connected to everything else, and the information is obtained almost in real-time throughout the world, there can never be too much emphasis on the importance of safety, cyber security and security for the future services provided in smart cities and intelligent societies.

4.5 New energy systems for arctic region energy purposes.

Because in the Arctic region are many places where is challenges to get energy when needed, here is presented one solution to use renewable energy systems there

[PIII][PV](Hanna Hoag, 2016) (Covernment of Canada) (Holdmann, 2017) (The University of Alaska Fairbanks). This solution also allows the power supply system to be out of reach of cyber attackers and hackers, as the system is local without interfaces to the Internet and the users of the system are local. In this system are also take care of also cyber security.

Figure 47 presents a test environment from hybrid energy system.
Description of the independent energy environment (test environment has been operating from 2009 to 2019 and still is working).

The location is Eastern Helsinki. The object is a two-story detached house. The house brush is east west. The roof has 48 pieces of 300 W solar panels (Behrang, Hamadani, Dougherty, 2014) (Damiano, Marongiu, Musio, Musio, 2013). The brush has a quiet 300 W wind turbine (patented). The 1000 Ah 48 V gel battery pack works with the 5 KW off-grid inverter. There is also an automatically starting gas generator that produces 5 kW of electricity and 5 kW of heat used with 11 kg gas cylinders. This structure tested independent production of hybrid energy without a power transmission network (Renewable Energy Institude). This kind of hybrid system can also be used in the Arctic region.

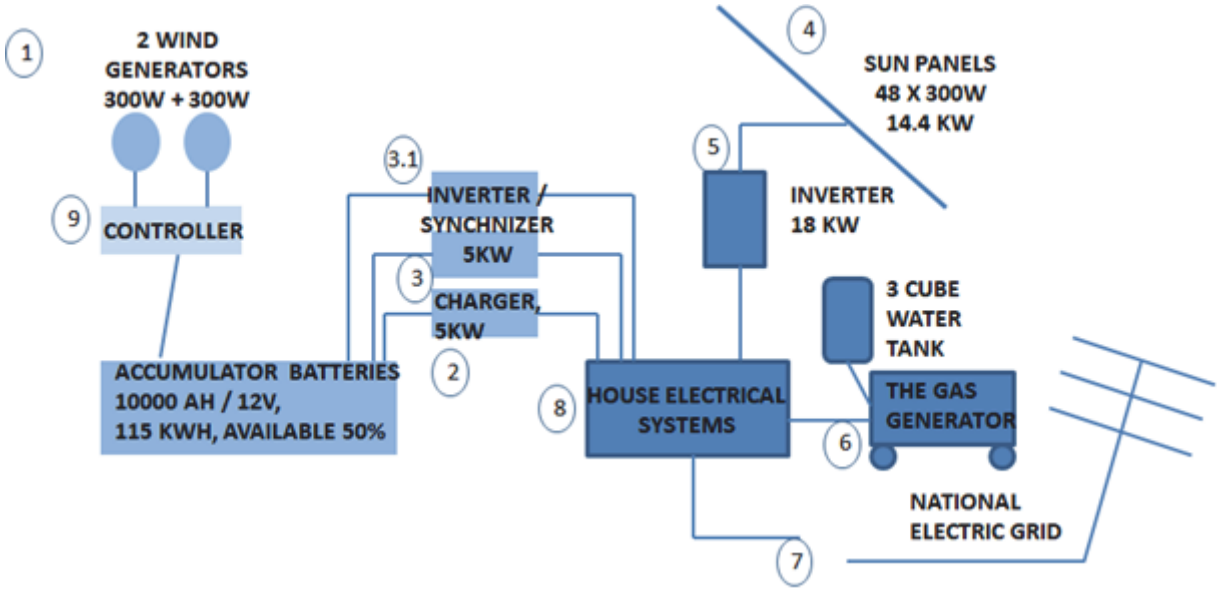


FIGURE 47. Test environment for renewable energy production in a private house.

The numbers in the figure represent the following:

1. The wind generators charge the batteries
2. Charger to complete charging
3. Overnight electric inverter which also synchronises the 3-phase panel supply

3.1 Test at 15 KW, was found to be too efficient

4. Solar panels

5. A panel inverter providing basic electricity
6. Gas generator starts when the other environment does not produce the required electricity.
7. National network disconnected
8. House electrical system
9. Charge control

4.5.1 Hybrid tests for solar panels

Solar panel orientation and best crystal structures were tested and developed between 2009 and 2012 (IEC 61646).

The results showed that the maximum energy of the panel is obtained when the solar radiation is perpendicular to the panels, and it decreases when the solar radiation angle changes from this perpendicular angle. For example, a 30-degree deviation reduces 30% of the perpendicular output of the panel. Single crystal panels make better use of side light than polycrystalline panels. The surface feature (orange surface) improves energy productivity in the side light. Panel warming significantly reduces energy output.

4.5.2 Conclusions for the installation of solar panels

As the installation of the sun panels should take into account the midday sun direction, panels should be added to the southeast and southwest of the building. This type of installation is maintenance-free and less expensive than swivel panels. If you are installing panels on the roof, a ventilation system is also needed. In maintenance technology, the mounting technology is made so that one panel can be removed from the centre panel without tools (the patent application from the method is ongoing).

4.5.3 Batteries, accumulators and converters tests 2012 and 2015

A lithium battery is the most effective for achieving the desired benefit (can be used as a power source long time). Other battery technology loses its charging power quickly as the number of charge cycles increase. Currently, the battery size is only economical when it replaces the average night-time consumption. The test was on-grid and off-grid and a combination of both batteries and devices and separate battery controllers. There was also a hybrid system for one device. Tested on both a nationwide network and a non-nationwide network. The hybrid system was working, but when it failed, you were without electricity. The best result is achieved if all energy sources have independent devices. If one goes wrong, the others will continue to work (Electro Power Systems, 2019).

4.5.4 The wind generator test.

The biggest problems were weather resistance, storms, storm gusts, snowfalls, rapidly changing wind directions and rotor sound. No satisfactory rotor model was found; thus, it was necessary to develop a new type of rotor to eliminate these problems. The rotor

type was tested in 2018 and proved to be working according to plan. This type of rotor is also currently awaiting a patent.

The hybrid solution has been tested since the summer of 2019. However, the real test will be the upcoming winter season, when we will be able to see if a house of more than 300 m2 has local power generation without using the national electricity grid to see how the planned design works in practice.

Observations

The production of solar panels energy began when the sun climbed over the forest border and ended when the sun fell below the forest boundary. Better total return was achieved when the solar panels were installed on the southern roof in addition to the eastern and western sides. The measured panel output power was 14 KW when some panels were moved to the ends. However, the benefits of the end panels came from the energy produced by the morning and evening sun, as daily energy production increased. Excess electricity was stored in batteries. It is currently possible to supply electricity to certain electricity companies in the Finnish electricity grid.

The spherical wind generator uses all wind, regardless of the wind direction. The generator output is stored in batteries. The battery is used with a 5 KW off inverter. There is also a gas generator which starts when the other energy output stops. The two-story detached house was heated or cooled by two air heat pumps, a ground heat pump and a generator cooling heat, which in part increases the energy efficiency of this house.

4.5.5 Dimensions

These energy calculations are based on a real basis calculation. It is not economically possible to store electricity for the whole winter. Theoretically, the total return on the solar panels in Helsinki is sufficient for annual consumption. This is based on the benefits of the morning and evening sun, when panels produce an average of 10 hours a day energy. The yield can be calculated for eight months per year, 240 days or 2,400 hours. During this time, the panels produce energy with a slightly more than 60% efficiency. Thus, in theory, the demand for electricity by a two-story detached house would be covered. However, storing electricity is not economically viable except for balancing the energy of the panels overnight. During the night, the energy consumption is minimised; for example, the heating is minimised (turned off), which amounts to about 2 kWh per 14-16 hours of consumption.

The power of the gas generator is worth half the efficiency of the solar panels and the grid inverter is half the power of the gas generator. The wind generator is a complementary power source and has the same power as the inverter, at 2-4 KW.

The system is also very economical and environmentally friendly as the only emissions are from the use of a gas generator. This solution is useful in areas where there is no national network, or it is too expensive to implement energy supply systems such as in archipelago cabins where only basic heat is maintained in the winter, in mountain areas or communication stations without protected energy systems, and in the Arctic region.

The corresponding test environment will be installed in a detached house in the eastern part of Finland where there are a lot of power outages. Energy companies in the

region are positively responsive to this type of renewable energy solution and encourage us to develop and supply extra energy to the grid for the residents of the region to utilise. Eastern Finland author has been using in his childhood home the air heat pump for over five years and is satisfied with its use. Another new test environment is to be built in a summer cottage, where it is possible to test the suitability and cost-effectiveness of the concept for smaller-scale energy production. Storing all the extra electricity generated by the panels would require cheaper technology than the battery. Theoretically, it is possible, but it is not economically sensible; by contrast, the gas generator is economically reasonable for use in (winter time). The heat of the gas generator can be utilised only when needed. The challenge is to come up with a way to store solar power in small production environments so that its full benefit can be used in the dark season.

In this test environment, renewable energy systems produce enough energy for a family house without requiring any connections to the national electric grid. Figures 48, 49 and 50 present the amount of solar energy generated in different months in the Tampere area and the wind energy generated in Jokioinen in Finland.

4.5.6 Used tests

Test environment:
House: Two floors comprising 200 m2 warm space. The heat distribution downstairs uses water circulation in the floor and upstairs has electric heaters. The living temperature is 22 degrees, with a backup system, with fireplace and oven. The house has free air circulation.

Outbuilding: One storey comprising 160 m2 of warm space, with underfloor heating, electric heating cables in floor casting and a target heat of 16 degrees. In addition, there are two greenhouses, each with a 1 kW electric radiator; the thermostat is set at 16 degrees and is used from May to October.

With purely electric heating, the average annual consumption was 65,000 kWh/year. When the fireplace and oven were used in the freezing cold times, the total consumption fell by 59,000 KWh/year.
Results of the tests:

Step 1:

A ground source heat pump was taken in the use, two rock wells, 120 m deep both and 10 m apart. Annual consumption thereafter was an average of 46,000 KWh/year.

Step 2:

Six air heat pumps, two upstairs and two downstairs in the house, and two outbuildings were added. In the air conditioner was taken in the use a heating recycling system, which also produced hot water. The annual consumption thereafter was an average of 28,000 kWh/year.

Step 3:

The greenhouses were equipped with air heat pumps, now running April to December.

Annual consumption thereafter was an average of 24,000 kWh/year.

Step 4:

Solar panels were taken in the use in the house roof, 14 KW panel field. The average amount of electricity paid is 13,000 KWh/year to the energy companies, and from April to September the panel yield covered the consumed electricity.

Step 5:

The wind generator tests were done with a self-developed special regulator, with a mean wind of less than 3 m/s with a wingspan of 2 * m2 and energy production was 3,000 KWh/year.

Observations and conclusions

By using our own batteries, we were able to save on electricity transmission costs. However, in the summer there was an over-production of electricity that could not be utilised. With a good electricity contract meaning price of energy, the result will be the same as that obtained without batteries.

The diesel generator can produce the missing heat and electricity, but this method is harmful to the environment. A gas generator is a more climate friendly method of supplying the missing heat and electricity. Because peak consumption occurs at a time when other renewable energy sources are scarce, the gas generator must produce 8 kW of electricity and the same amount of heat.

Winter frosts are a challenge for local energy production in inland areas where there is no wind. High masts are a possible solution in sea and mountain areas, where the winds can compensate for the lack of energy. Allowing the distribution of electricity between small areas (i.e. dismantling of electricity distribution monopolies) would facilitate a solution to the problem during peak energy consumption.

4.6 Background information

Background information from sun radiation and wind energy in Finland at different times of the year and in different years (Flink, Tampere).

The sun and wind energy and the availability of sun and wind energy at different times of the year was studied in Finland nearly ten years and the results obtained were compared with those elsewhere in Europe, in Freiburg. The PVGIS geographic information system, which is a tool for geographic assessment of solar energy availability, was used to estimate the availability of solar energy (Photoelectric Geographic Information System). It contains two databases, one covering the whole of Europe and the other covering the Mediterranean, Africa and south-west India. The European database is based on measurements of 566 weather stations taken between 1981 and 1990. The whole area under investigation is divided into 1 km x 1 km squares that compute horizontal solar radiation based on measurements from the nearest weather stations, terrain features and weather statistics. The PVGIS system is also used to calculate incoming solar radiation at different tilt angles, but it is not possible to change the direction.

The results show that the average daily accumulation of solar radiation in southern Finland, despite its northern location, is almost the same as in central Europe. In Tampere, for example, solar radiation is only 10% lower than in Freiburg (Figure 48)

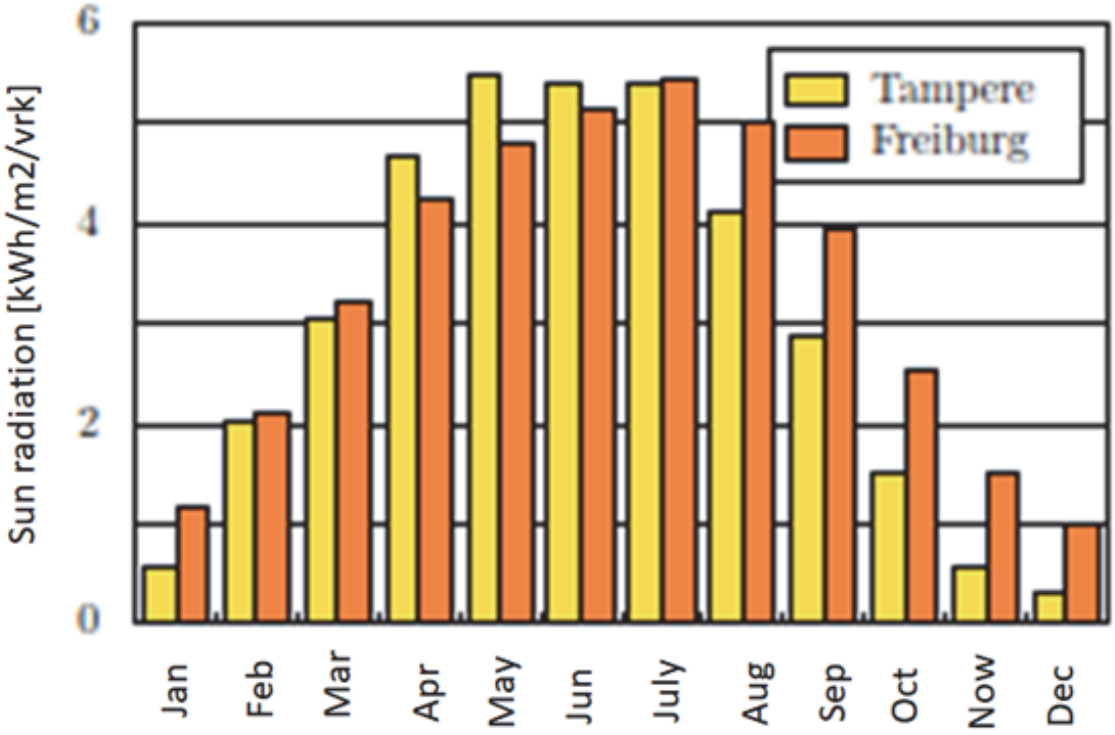


FIGURE 48. Average daily accumulation of solar radiation in Tampere and Freiburg.

Figure 49 highlights the variation in monthly solar exposure in Tampere and Figure 50 shows the monthly wind energy density based on the Finnish Wind Atlas in Jokioinen.

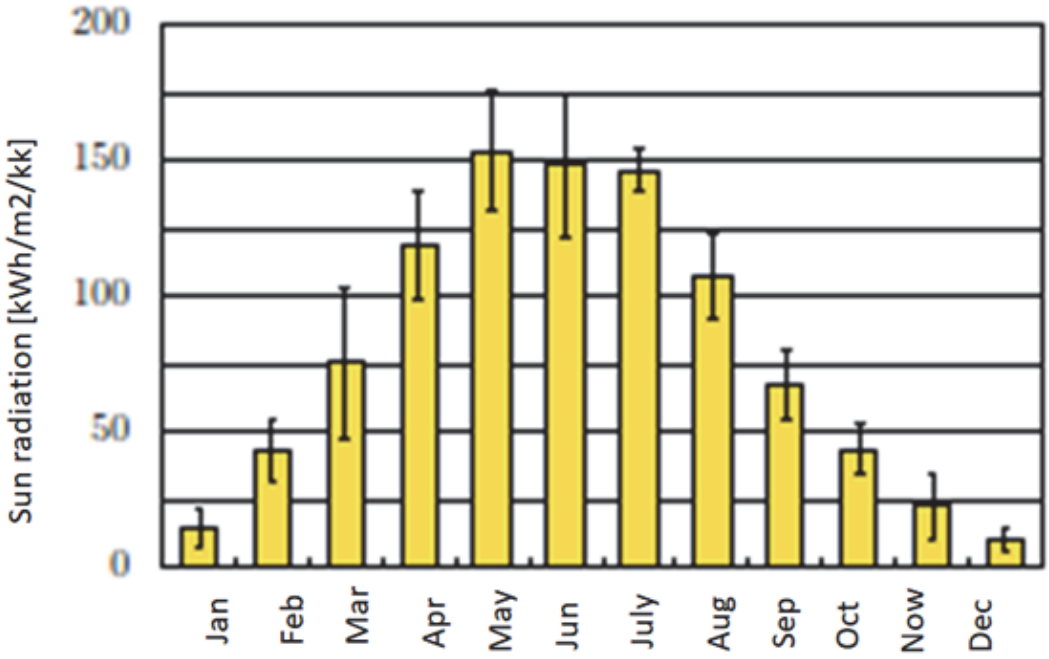


FIGURE 49. Variation in monthly solar exposure in Tampere.

The range shown at the top each bar depicts the standard deviation calculated from the variation in the monthly accumulation of solar radiation variations in different years.

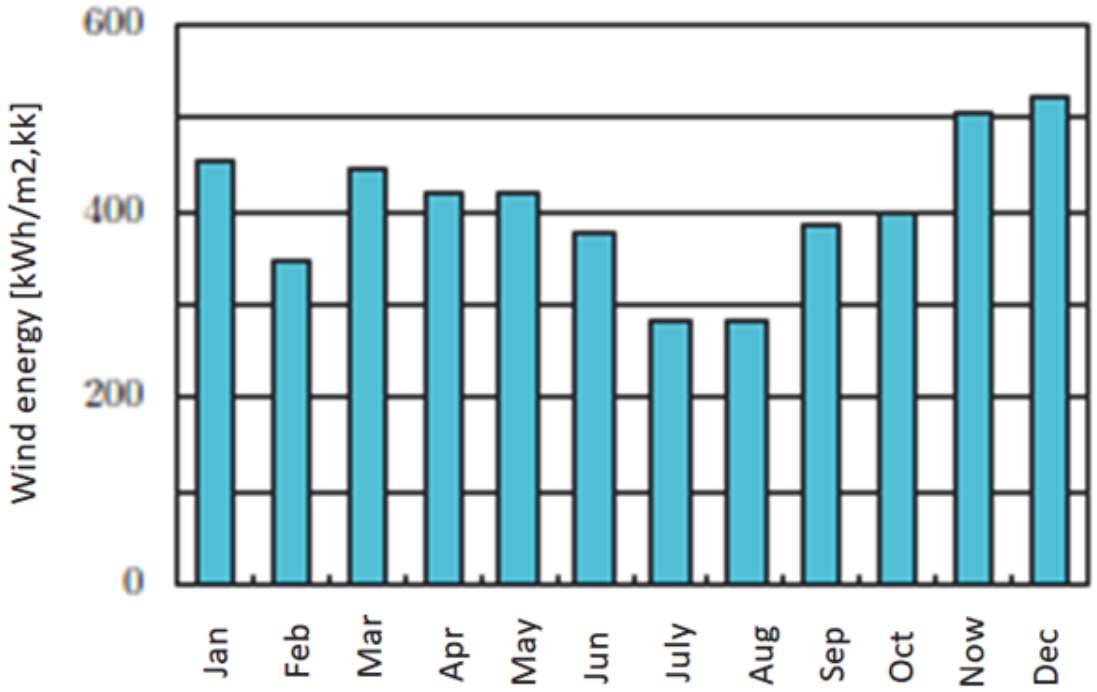


FIGURE 50. Monthly wind energy density based on the Finnish Wind Atlas in Jokioinen.

Monthly wind energy density measurements were made at 50 meters above ground level. Given information shows that we can use a renewable energy system to produce enough energy in northern areas in Finland and it is possible to use the system in the Arctic region. Hybrid solutions can also help to protect our energy systems from cyber-attackers because they provide connections to the internet and other communications networks.

4.7 Technologies in the Arctic region

4.7.1 Example of energy efficiency solution to the Arctic region

Energy efficient solutions affect small buildings such as homes, outbuildings and summer cabins (at least in Finland) because of the long distances from electricity distribution points, the reliability of energy supply and the cost. An example of a small unit that is suitable for homes in the Arctic region is an energy system that incorporates solar power, wind and thermal energy as a hybrid energy system (Figure 47). This hybrid energy system, as shown in Figure 47, has been tested in Finland for ten years near the Arctic region. Solar panels are installed in the small building, depending on where the sunlight best hits them, considering the sun's direction at different times of the day and at different times of the year in the Arctic region. Solar panels can be installed on all sides of the building's roof to provide the maximum benefit throughout

the day. It also possible to build some parts of small buildings such as homes below ground level so that in wintertime or in cold weather the wind would not impact the building directly and thus affect the temperature inside the building. This kind of concept raises opportunities to develop energy efficient solutions for smart home infrastructures in the Arctic region (Figure 51).

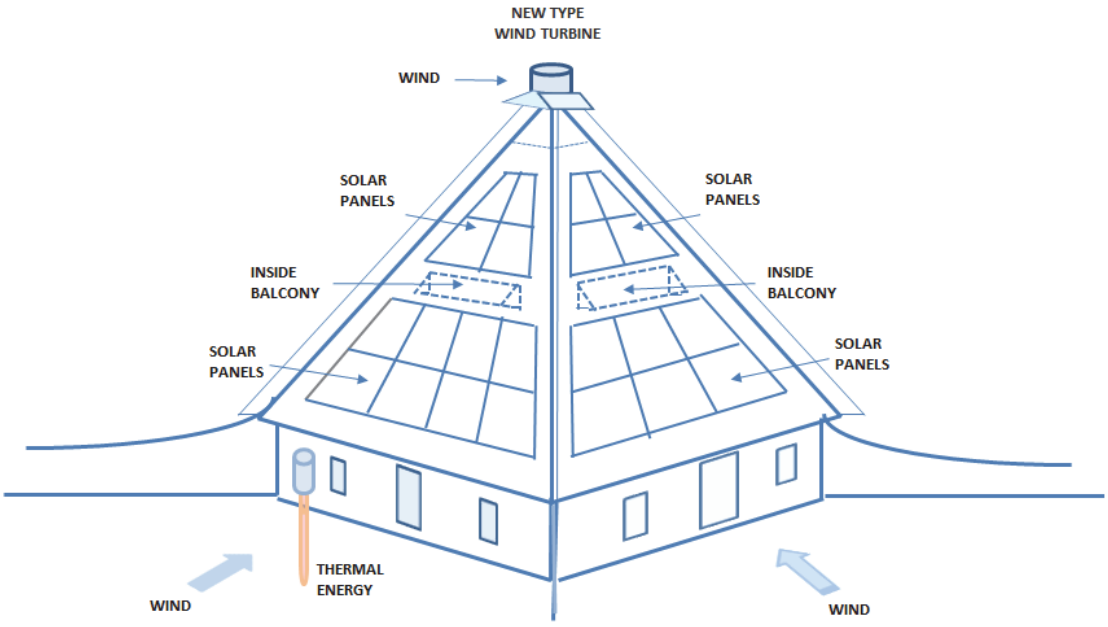


FIGURE 51. An example of a possible arctic energy system in a small structure.

As Figure 51 shows, the house uses solar, wind and thermal energy systems, which work together as one hybrid energy system.

It is also possible to install a small wind generator (see Figure 52) on top of the roof either alone or in a wind generator group. In the device shown in Figure 52, the flaps are an orbiting sphere on the surface of the cone and the generator has a cone inside. This type of wind generator is awaiting a patent.

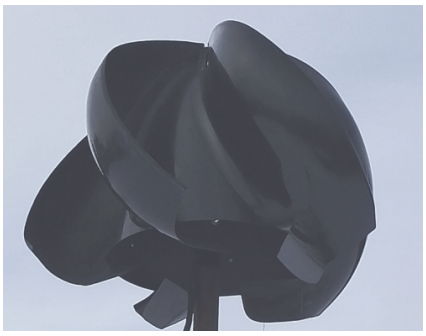


FIGURE 52. Small wind generator for the roof of a house (0.3 kW, 1kW or 2 kW,…).

4.7.2 Mobility in the Arctic region

Figures 35, 38 and 39 illustrate the various transport opportunities, such as public transport (trains, buses, air transport, ships, etc.) in the Arctic region. The citizens of the Arctic region need to know when this transport system can be used, when the vehicles arrive and depart and where you can buy tickets. These services must also be currently available to the citizens in the Arctic region. Because the distances are great and traveling from place to place is not easy, it is important to use a good communication systems to provide such services to the people located there.

4.7.3 The communication systems of the Arctic region

This chapter's part information is presented in chapter 2 ` Cyber Threat Analysis in Smart City Environments` and chapter 3 ` Undersea optical cable network and cyber threats` in this dissertation. There are presented top level principles (PI, PII, PIII and PV).

4.7.4 The satellite systems of the Arctic region

One potential idea for establishing communication in the Arctic region is the use of different satellites systems, although geostationary satellites do not suit this purpose well. Figure 53 shows the orbits of different types of satellites around the earth and their heights.

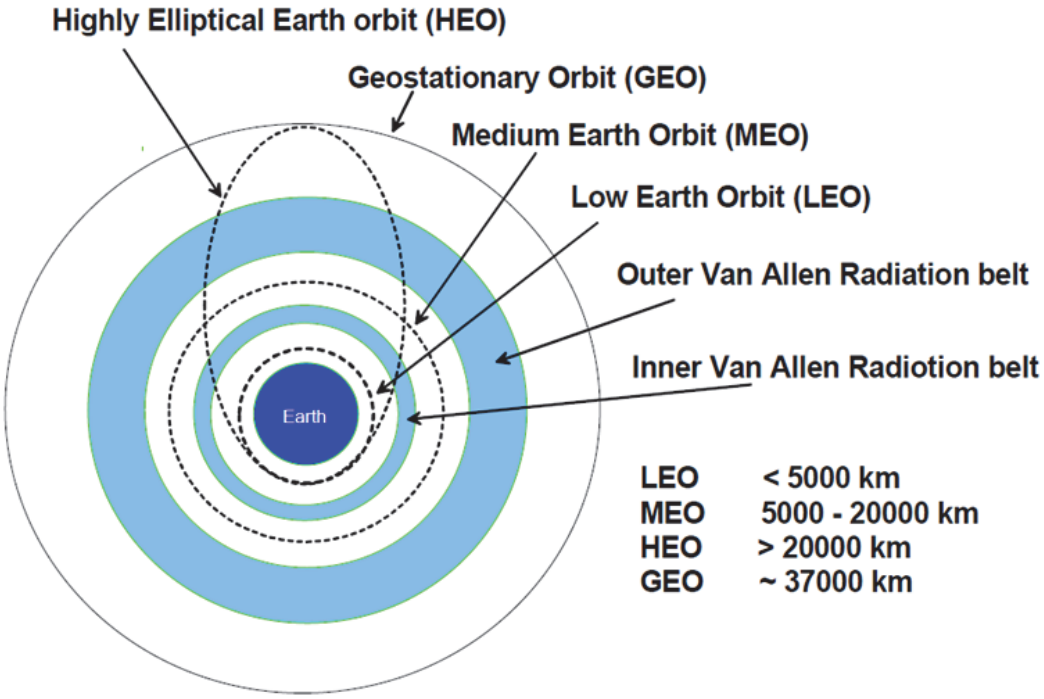


FIGURE 53. Satellite orbits (Hummelholm, S-72.4210).

1. LEO (low earth orbit) < 5,000 km – the period of this type of satellite is about 2 - 4 hours.
2. MEO (media earth orbit) 5,000 - 20,000 km – the period of this type of satellite is about 4 - 12 hours.
3. HEO (highly elliptical orbit) > 20,000 km – the period of this type of satellite is more than 12 hours.
4. GEO (geosynchronous equatorial orbit) are located about 37,000 km above the earth's equator and follow the direction of the earth's rotation.

The Van Allen radiation belts – where energetic particles such as protons and electrons are confined by the earth's magnetic field – can damage the electronic components of the satellite. Space debris belts – where spacecrafts are abandoned at end of their lifetime – are another obstacle. Such spacecrafts are becoming an increasing problem to the international community as they can cause damage to satellite networks and even to future space missions.

To provide services at the right place and at the right time over such a large area, the author has segmented the Arctic region's services into different segments (see Figure 44; infrastructure, energy, buildings and homes, mobility, telecommunications, and public and private services). Each set of operations has its own service and communication needs depending on the user group. Such groups include the indigenous peoples, immigrants, people living in the area, tourists, design and maintenance personnel, financial staff, telecom and service operator's staff, virtual service providers and operators, and administrative actors.

We must take into account the different needs of the different use cases and identify the needs of the people, businesses and regions, as well as the cooperative (coordination) needs of different states and interest groups. Each group of users operates horizontally in their service sector, as seen in Figures 43 and 44.

All of these groups will need means of communication that is different to what is currently available in the Arctic region. The communication services needed by these individual user groups will also differ from each other. Many groups need high bandwidth communication links which are not currently existent north of around 80° latitude. There will also be a need for highly trusted communications links for services such as e-health systems, and redundancy (protected connections) might also be needed. A satellite link could be used to provide such services. A satellite communication system is now days the only viable solution for communications with high data rates in the Arctic region (Birkeland, 2014). This level of data communications services would be developed with satellite communication systems that cover the Arctic region (Figure 54).

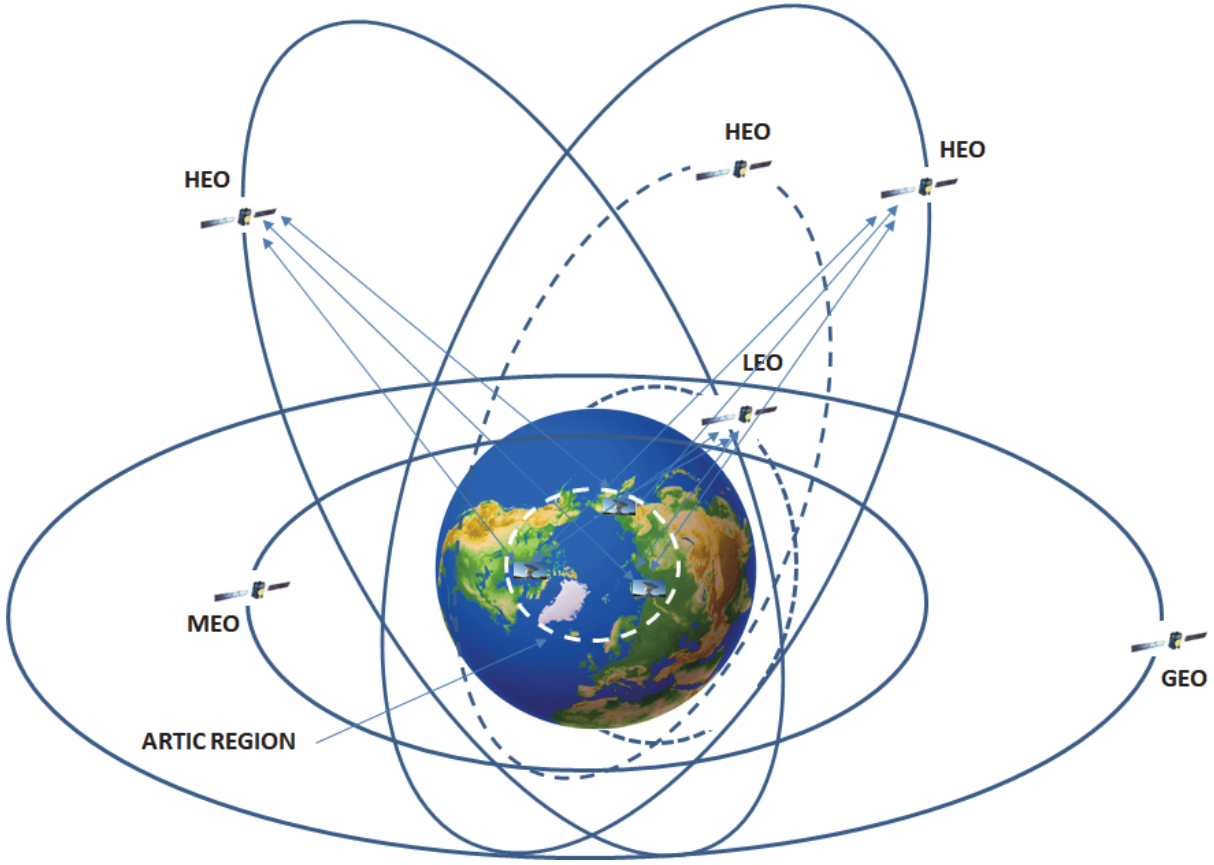


FIGURE 54. The Arctic region satellite systems.

Norway, Sweden and Finland have large populations living above the 65° degree latitude line that require high level connectivity to sustain modern services in their everyday lives.

4.7.5 HAPS for wireless communications.

The concept of HAPS, shown in Figure 55, has been known at the theoretical level about more than fifteen years (Aarne Hummelholm, S-72.4210) and is a proposed solution for the Arctic region's communications systems and service needs. Such a system can cover an area of about 400 km and provide connectivity in that area for various devices (mobile or fixed systems). A HAPS system can form a mesh network with other HAPS systems and with satellite systems. In this way, the HAPS system can provide protected communication paths if needed. Currently, the HAPS system life cycle is about five years, after which it must be regenerated. However, it is possible to take it down earlier for system updates. The HAPS system is quite flexible.

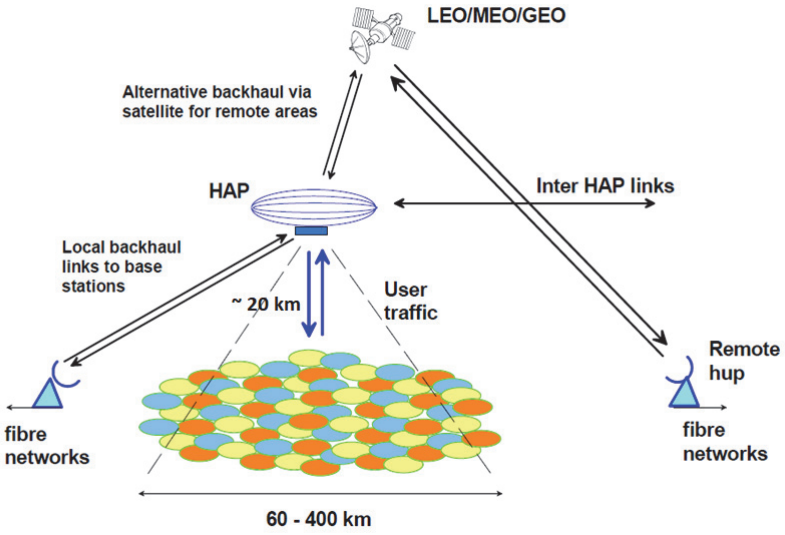


FIGURE 55. HAPS for services (Hummelholm, S-72.4210.

Combining the HAPS system with satellite systems makes the deployment of 5G systems in the region possible, wherever high capacity mobile services in the Arctic region are needed. By implementing this solution, we would negate the need to install long optical cables systems in the area, unless they are needed for some other reason. Nor do we need to install a large number of base stations in these areas, make communication stations and masts, or install long power lines or maintain roads in the wilderness, which will also conserve the natural wilderness. We can use local base stations if more communication connections to the HAPS systems are needed to provide services to the smart society in the region. It is also possible to make connections to the satellite networks in that way, as well as to the services offered by broader society. The Radio and TV transmission systems can also be installed in the HAPS systems, which would thus enable programs to be broadcast at lower power levels than is possible when using the current solutions.

When we use the HAPS systems, it is also possible to use 5G technology in a virtualised manner, so that only one operator manages the HAPS systems and its devices and it offers the services through a virtual operator. This also means that these virtual operators do not have to build their own communication systems in the region, which thus saves a large amount of money and energy, protects the environment and reduces the carbon footprint significantly.

We can look at this HAPS system as a cloud service concept, where the servers inside the data centres are virtualised. These virtualised infrastructures are offered to many virtual service operators, providing the resources they need; the virtual operators then provide their services to customers in these environments. This method can be used in future communication systems, comprising one infrastructure operator and many virtual operators. This concept would save investment money up front and reduce the maintenance and operating resources required later on (one observation).

Using networks between HAPS systems with links through satellite systems means these networks can be accessed from anywhere in the world, i.e. all services can

be made available through these arrangements to the Arctic Region, or elsewhere in the world. The HAPS systems can thus be used in many regions of the world where there is no established infrastructure, such as the countryside, developing countries, coastal and marine areas, border regions and desert regions, making it possible to provide the people living in these areas the services they need (one observation).

When installing the long submarine optical cable system in the Arctic regions, the SOC and NOC can be connected in the different areas to provide situational picture information to other service providers and to ensure cooperation in Arctic region. This concept would facilitate communication for more precise disaster planning and emergency response for public safety needs such as search and rescue. This setup can also be used to (1) allocate scarce resources more effectively between the different country's security authorities and (2) provide opportunities to support scientific research by supporting researchers' access to information, ability to share scientific resources and instruments, and virtual collaboration with colleagues around the world.

4.7.6 Citizens connections to services in the Arctic region

In the Arctic regions, as in other areas around the world, service and communications operators will provide a wide range of services available to citizens in real time, regardless of location or time (Figure 8). From this foundation, the data streams between the active nodes can be formed in the same way as they are elsewhere in the world. These active nodes can be user terminal devices that exchange data directly between themselves, D2D traffic, wearables, HUBs using wireless technology as a part of active node communication, IoT devices and M2M devices. In the illustrated concept, almost all devices use wireless technology for mutual communication and in communicating with telecommunication networks and services. Active nodes can form groups and subgroups where the data is classified into different levels of protection: public, restricted, confidential, secret and top secret levels. This classification has to be taken into account in both wired and wireless networks from building and apartment structures to virtualised networks and data centres and virtual environments from the user terminal to the entire service chain from beginning to end. In the future, telecommunications systems and services will also be working in a virtual operating environment, where the resources of telecommunication networks and data centres are shared among users of networks and services by the orchestration of different service operators, either together or separately. These virtualised systems could work on wireless or wired networks, as seen in Figures 8 and 9 presented earlier in this dissertation.

As the latest technical concept, this virtual network and service environment will use slicing, which groups the various services according to the quality and criticality required by the service or according to a specific group of users (see Figures 9 and 10).

Future environments will require a many different levels of integration, orchestration and federation for the services to function in the desired and flexible way. It is therefore necessary to manage the users of services, the users' access to management services, the management and control of common, infrastructure, and financial services, and the management of sliced service groups of virtualised networks (Figures 9 – 10). In this scenario, we will also see how the user's terminals are connected to the networks

and services. Documents PI and PII explain how citizens connect to services in the smart cities and in the Arctic region in future environments.

4.7.7 Public and Private services in the Arctic region

The public and private services in the Arctic region are associated with many developing aspects such as real-time, digitalisation and environmental changes, changes in service provision, international cooperation and competition, conflicts of interest (international, regional, national, local), changes in lifestyles, increased pressure on service provision, infrastructure, urbanisation, environmental pressures, political climate, interest groups, refugee problems and climate change.

Another requirement of this future Arctic environment is that we need to be sure that the citizens' data are properly protected in accordance with the regulations in the registers and that the registry holders protect the citizens' information kept in their registers. They should demonstrate that the data retained is protected in accordance with the laws and regulations and, if necessary, be revised in practice in European areas (EU-GDPR, 2016) (EU-MDR, 2017) (EU-NIS, 2016).

The EU-GDPR directive in brief:

> The General Data Protection Regulation, in turn, obliges the organization to identify risks when defining technical and organizational measures to ensure the protection of personal data. Technical and organizational measures include, for example, instructions given to staff to implement data protection, self-control through access control, information system security, data encryption, and other security measures. Risk assessment is a continuous activity: the adequacy of the measures in relation to the risk involved in the treatment must be continuously evaluated and updated as necessary. The controller, in this case the healthcare organization, also has a duty to demonstrate a risk-based approach. The EU Data Protection Regulation introduces risk management and reporting obligations[3].

The EU-NIS directive in brief:

> Network and information security (NIS) directive is created to ensure a high level of security of network and information systems across the Union. According to the Directive, key service providers for example heath care and certain digital service providers are required to manage comprehensive network and information security risks and report to the responsible authorities any security incidents that hinder or threaten the continuity of operations[4].

[3] Jenni Siermala, SoteDigi-Finland, 2019.
[4] Jenni Siermala, SoteDigi-Finland, 2019.

The EU-MDR directive brief:

> Medical device regulation (MDR) requires using only devices defined by the regulation for treatment, diagnosis and measurement of the patient. The responsibility of the medical device manufacturer covers the entire product lifecycle from design to exit from the market. The manufacturer is thus responsible for the entire lifecycle of the medical device, the application, interfaces and security as well as unqualified standards. The medical device manufacturer must monitor the product on the market and collect feedback on the use of the equipment. If there is a product risk in the feedback, the matter must be corrected immediately. However, according the MDR, the manufacturers shall set minimum requirements for hardware, network features, and security measures, including protection against unauthorized access, as required to use the software[5].

The content of the directives is reflected in the national legislation of the European Union.

4.8 Natural threats, accidental threats and cyber threats

4.8.1 Infrastructure-related threats

Typically, infrastructures management and control systems, such as electric power stations, big buildings and homes, are connected to the internet. This kind of management and control system forms a service network on the internet, but security that is too low level leaves them vulnerable to attacks by hackers and cyber-attackers. Many service operators of building automation systems connect their control and management systems to the building automation systems remotely via the internet, which are their responsible. Vulnerabilities in the connections enable attackers to penetrate the systems and cause harm to the systems which are used every day.

Long-distance electric power transmission lines are controlled by radio communications (wireless) systems, which also involve security challenges. These control systems are also quite easy to disturb and provide an easy way for hackers to enter the power supply management system and interfere with functions or even block the operations altogether.

4.8.2 Satellite System Threats

The satellite system uses different radio frequencies from the ground stations to the satellite and from the satellite to the ground stations (Figures 8, 54 and 55). These frequencies are quite easy to disturb and even hinder altogether. Satellite location information that provides positioning information can be changed to show the wrong coordinates, which can cause considerable harm to the sea example navigations information is not right and ships goes wrong way or wrong places. A shipping service (Vessel Traffic Service = VTS) is needed to help ships in such situations, and if the

[5] Jenni Siermala, SoteDigi-Finland, 2019.

systems are down for one reason or another. VTS system keep track of vessel movements and provide navigational safety to the ships

4.8.3 Communications System Threats

The communication systems in the Arctic are interconnected by a national communications network, which allows connections to the continent's communications networks. Once these connections have been made, the Arctic communication systems also become a target for hackers and cyber-attackers. Mobile technologies such as 2G/3G/4G are currently used in the Arctic region.

4.9 The threats associated with the submarine optical cable systems in the Arctic region

This chapter's part information is presented also in chapter 3, `Undersea Optical Cable Network and Cyber Threats` in chapter 3.7. ´Natural threats, accidental threats and cyber threats´ and in chapter 3.8. ´The making and modelling of a threat analysis´ in this dissertation (Threats to Undersea Cable Communication, 2017). But this is important part of Arctic region communications systems. There is presented top level principles. Table 12 shows the differences when looking at the threats in different segments. We need to take into account the upper level conceptual threat matrix for the segments shown in Table 12 when designing and developing undersea submarine optical cables systems in the Arctic region.

TABLE 12. Upper level conceptual threat matrix for submarine cable segments (PII, PIII, and PV).

SUBMARINE CABLE SEGMENT THREAT	LAND AND BEACH AREA (Seg. 1)	NEAR SHORE AREA ~50 M (Seg. 2)	OFF SHORE AREA ~ 50 – 100 M (Seg. 3)	CONTINENTAL SHELF ~ 100 – 200 M (Seg. 4)	DEEP SEA ~ 200 M + (Seg. 5)
NATURAL THREATS					
SHARKS					
EARTHQUAKE					
LANDSLIDE					
VOLCANO					
TSUNAMI					
ICEBERG					
OCEAN CURRENTS					
ACCIDENTAL THREATS					
FISHING					
ANCHOR DRAGGING					
DREDGING					
MALICIOUS AND UNDERSEA WARFARE					
CYBER ATTACKS					
VANDALISM					
ACTIVISTS					
THEFT					
TERRORIST					
STATE-ACTORS					
UNDERSEA WARFARE					

Note. Upper level conceptual threat matrix for submarine cable segment (Threats to Undersea Cable Communications, 2017). Threat impact level is shown as colours: Green = Low; Yellow = Medium; Red = High.

4.10 The making and modelling of a threat analysis

Cyber attackers, hackers and terrorists can also use AI to search for vulnerabilities in submarine optical cable systems through which they can penetrate the systems and services and attack data centres on different continents. There are many ways that cyber attackers can hack into a submarine optical cable system to gain access to its managements and control systems.

Figure 56 presents the threat probability tree model for the Arctic connect cable system, which can be used for developing the threat model.

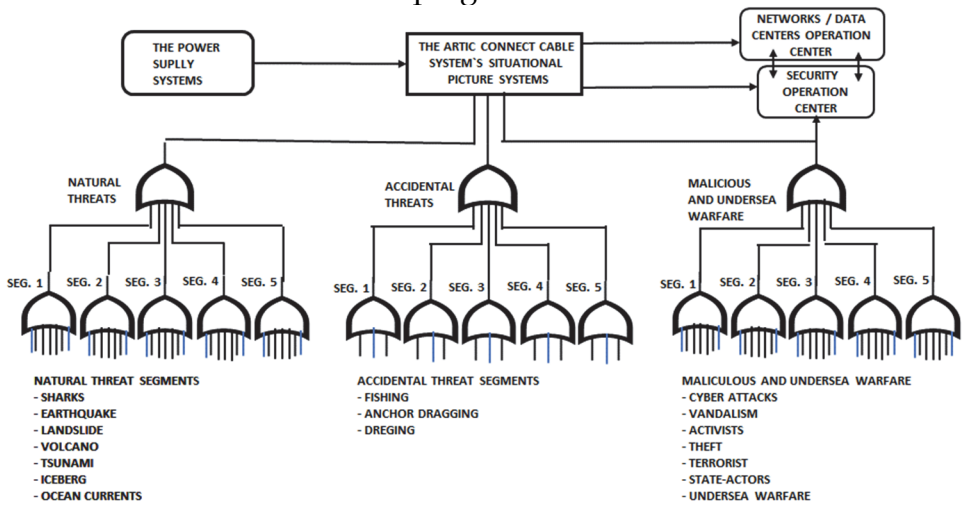


FIGURE 56. An example threat tree model for the Arctic cable system (PII, PIII, PV).

TABLE 13. Meaning of Notations

ACTION	EXAMPLES	NOTATION
THREATS OR ATTACK	SUDDEN EVENT, ACCIDENT, TAPPING, EAVESDROPPING, SNIFFING, SCANNING, …,	A
DETECTION	ALARM INFORMATION, SYSTEMS MANAGEMENT INFORMATION, INTERNATIONAL INFORMATION, …,	D
COUNTERMEASURE	ANALYSING OF THREATS AND VULNERABILITIES AND TO REPAIRING, SAFEGUARDS PUT IN PLACE, …,	M

Threats (P(t)), probabilistic treats or attacks that will occur

$$P1_{S1\ldots7}(t) = P1_{A1\ldots7}(t)\,(1 - p1_{D1\ldots7}(t))\,(1 - p1_{M1\ldots7}(t)), \quad (1)$$

to seven different types of natural threats;

$$P2_{S1\ldots3}(t) = P2_{A1\ldots3}(t)\,(1 - p2_{D1\ldots3}(t)\,(1 - p2_{M1\ldots7}(t)), \quad (2)$$

to three different types of accidental threats; and

$$P3_{S1\ldots7}(t) = P3_{A1\ldots7}(t)\,(1 - p3_{D1\ldots7}(t))\,(1 - p3_{M1\ldots7}(t)), \quad (3)$$

to seven different types of malicious and undersea warfare.

$$P1_{S1\ldots7}(t) = [(P1_{S1}(t)) + (P1_{s2}(t)) + \ldots + (P1_{s7}(t))], \quad (4)$$

information to the situational picture systems.

$$P2_{S1\ldots3}(t) = [(P2_{S1}(t)) + (P2_{s2}(t)) + (P2_{s3}(t))], \quad (5)$$

information to the situational picture systems.

$$P3_{S1\ldots7}(t) = [(P3_{S1}(t)) + (P3_{s2}(t)) + \ldots + (P3_{s7}(t))], \quad (6)$$

information to the situational picture systems.

Table 9 is divided into different segments according to the depth of the submarine optical cable system, and those segments are further divided into different categories of threats. We can calculate the probability of a threat in every segment based on information obtained from international research reports, from the ESA, from the Arctic statistics from National Aeronautics and Space Administration (NASA), from sensors and sonars, and from news concerning natural or animal events, accident or injury cases, and cyber-attacks in terms of how many times they occur, in what areas and at what time of year. This threat probability calculation can done for the full length or just a part of the cable system. For the overall situational picture, we also need information about status of the power supply station.

Figure 56, the Situational Pictures System, has a unique icon for each threat type that tells the situation of the Arctic connect cable system in different segments and regions. The situational picture information is also sent to the SOC and NOC and to the data centre management systems in different areas. These situational picture data should be made available to the various Arctic network operators and service providers, since the response times should be sufficiently rapid to allow, for example, rescue operations to be started as quickly as possible. The situational picture of the Arctic connect cable system information is also sent to the cable operator's operational centre.

The land and beach areas of submarine optical cables systems are the easiest for attackers to penetrate. When using large capacity systems in an undersea environment, and new types of modulation technology in those systems, the best possible cable tapping points for cyber attackers are after every OA in deep underwater areas. This offers the attackers various opportunities to obtain a large amount of information from

different companies, organisations and governments. In this situation, cyber-attackers and hackers can obtain IP addresses from these companies, organisations and governments and conduct DDoS, ransomware or malware attacks. Ransomware attacks are typically carried out by using a Trojan to enter a system through, for example, a vulnerability in a network service. One possible cyber-attack model is that of an APT, which is a targeted cyber-attack in which an intruder gains access to a network and remains there undetected for a long time. APT attacks typically target organizations such as national defence, manufacturing and the financial industry, and companies that deal with high-value information, military plans, and other data from governments and enterprise organisations. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause direct damage to the network or organisation.

As Figures 28 and 29 in Section 3.7.2 illustrate, if attackers are able to join the optical submarine optical cable system, they will also have access to management system, and thus have the opportunity to use them for their own purposes. For example, they can change the ROADM unit configurations to meet their requirements. We also need to carefully consider the power supply system to prevent attackers taking advantage of any vulnerabilities. As Figure 22 shows, for communications networks between different smart cities in the future, we must also consider communications inside the cities, as many challenges stem from the operating environment and from heterogeneous telecommunication networks, where new devices and systems, including IoT, D2D, M2M and V2X systems are seamlessly interconnected with peoples' smart devices. These systems have expanded into homes, building automation systems, cars and various control and energy systems, and people use their smart devices everywhere in the Arctic region. These smart city systems also need specific applications, which are stored in the Data Centre, as shown in Figures 8 and 10. Using these specific applications means also that hackers, terrorists and cyber attackers have many opportunities to find vulnerabilities in the Arctic region to attack its smart city applications and services. The interconnection between data centres would also allow the hackers and cyber attackers to attack services and service systems located on other continents.

4.11 Answer to the research questions, conclusions and future work

Answer to the research questions

RQ 3: It is somewhat difficult to provide communications services to all citizens in the Arctic region because it covers a large area and it is expensive to develop and install fixed communications systems. The author presented the HAPS system which can connect to satellites and base stations in the area. The Arctic region communication systems are typically based on submarine optical cable systems, where they are installed. The HAPS systems provides opportunities to integrate the communication system of the Arctic region. Satellite systems are difficult to use in the Arctic region because the region is outside of the satellite coverage area. While the HEO satellite system could be used, only one country uses that system there.

RQ 3.1: The author presented a new type of building for the Arctic region (Figure 51), where part of building is below ground level and uses sun panels, wind generators and ground (or geothermal) heat in a hybrid mode. It is also possible to use a CO_2 and greenhouse gas elimination system.

RQ 3.2: Figure 46 presented the future office building with infrastructure and communications systems and with one floor below ground level. The building has sun panels and wind generators on the roof and CO_2 and greenhouse gas eliminator systems inside.

Conclusions

The system to be built in the Arctic region is technically very complicated and many new technical solutions will be needed to meet the required transmission rates and the usability, quality requirements and criteria. This places considerable demands on the management and control of the system and on the organisation of its maintenance. The design should take into account the long life cycle of the submarine optical cables. Changes in social structures take place very quickly and will affect the implementations and operating models (Figure 45). The current powerful digitalisation trend increases the range of services offered and facilitates their easier use. These developments also have a strong impact on the service chains for the provided services, including the subcontractors with their subcontracting chains, the hardware solutions, the service providers and the operating models in every part of the service chain on every continent.

Currently, and in the future, modern communications systems connect data centres and data networks on different continents, enabling real-time communication throughout the world. This type of communication is made possible by undersea optical cable and satellite systems, which we use for daily communications. Because submarine cables systems have had such large strategic impact on our society, they are also a tempting target for hackers, cyber-attackers, terrorists and malevolent state actors who seek to gain access to the information being transmitted through the cable networks between the continents. When considering cyber security in the systems design, we must take into account the upcoming technologies because changes in cable technology due to dispersion phenomena make it difficult to detect intrusions into the cable system.

Future work

Because communication systems are such critical systems that are used by a number of different countries, organisations and individuals, it is essential to examine the key issues affecting the functioning of the system.

- In relation to cyber safety, the use of machine learning needs to be investigated and its potential to protect submarine optical cable systems and satellite systems needs to be investigated to better protect against malware and cyber-attacks.
- The use of COTDR should be investigated because it is used to search for faults and to detect the tapping of cable connections.

- We must investigate the different protection mechanisms of submarine optical cables systems because they are extremely important to the central fibre optic connection between different continents.
- The effect of different encryption systems, such as quantum encryption and or Layer 1 - 2 encryption systems, should also be tested.
- The virtualisation of telecommunications networks and data centres should also be considered to ensure the security of services offered in the Arctic region.

CHAPTER 5. E-HEALTH SYSTEMS IN DIGITAL ENVIRONMENTS

This chapter is based on publication 'E-health Systems in Digital Environments' and additional materials from author earlier works. Publications VI and VII extend and deepen the content of the chapter.

5.1 Introduction

As we live in the digital world, people can be provided with more effective treatment methods that allow them to live longer and better lives in their homes, including better home care and preventive health care. People can easily carry portable sensors and intelligent devices in their bodies and wrists that relay their vital information to hospital systems in real time, allowing healthcare staff to track human vitality in real time.
Although the digital world offers opportunities to improve our healthcare systems and make the analyses of diseases more effective, different devices and systems may not work well together; almost every manufacturer has their own technical solutions that work only in certain environments.

Therefore, there is a strong need for unified concepts and IT platform solutions in healthcare systems. The technology currently in use is very varied and while international standards concerning healthcare systems and devices are being developed, they are not yet ready. In addition, the technical and functional requirements for telemedical communications systems and equipment, as well as the requirements for providing secure data transmission in remote medical care are lacking.

In the news, we often see and hear about many medical devices that have caused damage to patients' health around the world (ABC news). There are also a lot of vulnerabilities in IoT devices and sensors, which raise security risks, cyber risks and the risks in the reliability of data.

This chapter discusses telemedicine solutions for the future of society. The chapter starts with a brief introduction about the equipment used in a hospital environment and at a patient's home. The main focus is the communication arrangements, consisting of the bio-signal formation of the patient's sensor and the flow of bio-signals to the hospital information systems for analysis and monitoring. This study examines the cyber threats

and attacks to e-health systems and what they mean for patients' health. This study also examines the authenticity, traceability, authentication and protection of privacy.

Today, hospitals and healthcare peoples want to exploit the potential of digitalisation in the services of health care, diagnostics and the analysis of diseases, in the precautionary treatment and in monitoring the progression of diseases. However, the rapid technological advances underlying digitalisation brings challenges for technical healthcare systems and for all health services. In addition, patient location information can be used only based on guidelines and regulations which are ministries responsibilities.

It is imperative that health services are available 24/7, regardless of time and place, and qualitatively and equitably, even if the patients are located in cities or in rural areas a long distance from the hospital or treatment point. In addition, patients' spatial data may be used to indicate an individual's whereabouts so that it is possible to warn healthcare persons as soon as possible and get help to the right place.

Although health care is looked at in terms of services and quality, cost-effectiveness has become increasingly important in the decision-making process. Cost-effectiveness also affects patient care methods and solutions. The goal is to organise treatments so that patients are in hospital for as short a time as possible, and they are sent home once the necessary conditions for arranging home care are in place.

One aim of digitalisation is to provide the patient with treatment so that they can be sent to home care without undermining the quality of care or adequate levels, even in the circumstances at home. However, doing so requires the introduction of new technologies and the integration of different types of transportable equipment, such as IoT, and various sensors and actuators, as part of the health systems. Together, this equipment produces a lot of information about the patient's condition and the environment in real time. These data are analysed in hospital systems, leading to the necessary treatment-related measures.

As the pace of development has been very rapid and new technology has been introduced very quickly, the international standard work, example IEEE and ITU-T, has not been involved in the development process. Some of the service providers' data centres provide manufacturer-specific solutions for IoT devices, sensors and data storage systems, as shown in Figure 57, which lead to a challenge when attempting to connect IoT devices to smart devices.

Smart devices can be connected to fixed or mobile networks to transfer the patient's bio-signal data to hospital systems, where the information is analysed. The care staff then make the necessary decisions based on the analysed results and give information about the management measures to the patients.

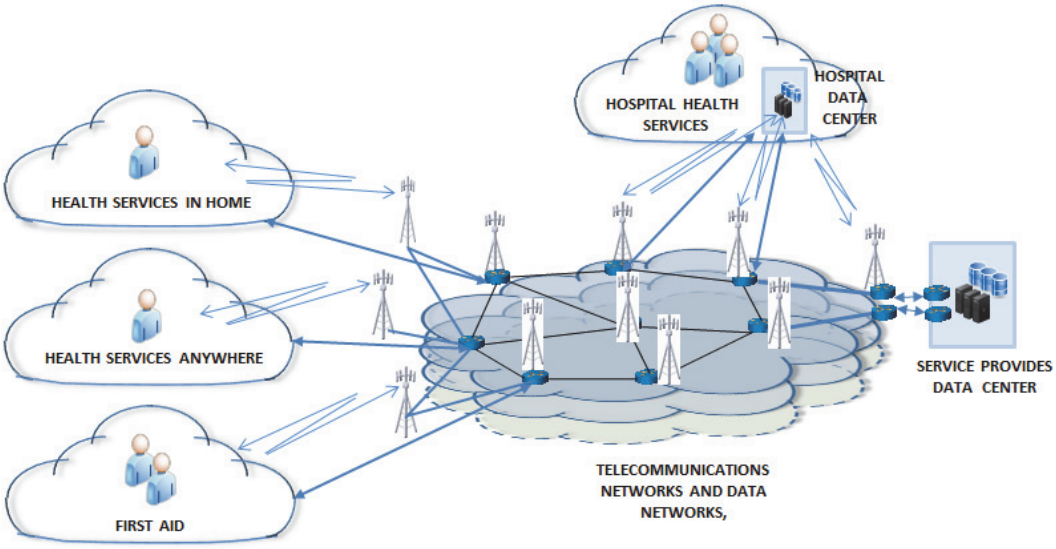


FIGURE 57. E-health top level architecture.

For many technical specifications, the situation is variable regarding specifications, and the terms used vary, depending on the speaker or the time in which the term is used. For example, the following terms vary slightly in importance: Telemedicine, telehealth, E-health and M-health and this means that specifications maybe varies also. This paper uses the terms E-health and M-health. However, this diversity of undefined terms is a source of challenges for security solutions, privacy and cyber security issues (Istepanian, Woodward, 2017).

E-health = The use of technology, electronic processing and communications networks for different healthcare services.
M-health = Mobile (smart) phone + healthcare delivery service.

5.2 Objective and grouping of chapter

To answer the research question, this study develops a model that facilitates cyber threat assessment and threat comparisons and facilitates threat analysis in an E-health environment. The results obtained through the model facilitates the design and implementation of architectural solutions. The model can be implemented to assess the cyber-threat scenarios of future telecommunication environments and their impact probabilities on E-health systems. The study draws on an E-health operating environment with a top-level architecture (Figure 58), where services and infrastructure are grouped into different use cases. The use cases are also divided into end-to-end communications segments, allowing us to analyse the vulnerabilities and define the cyber threats to various devices, services and information systems. Doing so enables us to more accurately define, evaluate and analyse the cyber threats in the whole system and obtain a better overall picture of the situation.

As shown in Figure 58, there are also several other viewpoints like communications connections to hospital outside data systems. An examination of threats can be made in

the various use cases involving patient wearables, sensors and IoT devices. When a patient or an elderly person is at home or outdoors using an e-health application on their smart device, they can also use other social services that are provided via telecommunications networks. This means that a patient or elderly person can connect to the e-health system in hospital or at home while also connecting to another internet or social media service. The exchange of information between the different service segments could pose a threat to healthcare systems and the entire e-health service. The networks of those service providers are used to integrate health data of patients or elderly people to the hospitals systems. We must examine this end-to-end communications path and all the devices connected to that path. The above-described integration accelerates at all levels of activity in each region both horizontally and vertically. Analysing the latest technologies and their services and applications in these smart environments will further complicate the cyber threat estimates. These considerations are important in the selection of the target area for which the final dependency analyses, cyber-threat assessments, risk assessments and analyses are made (PIV).

Section 5.2 presents the ecosystems and collaborative environment formed by active nodes as well as an architecture model that describes the interfaces of the current operating environments of the hospital, the home, outside the home, telecommunication networks and hospital data centre at the general level. The virtual environments management and control and telecommunication networks and data centres is part of this whole. Section 5.3 describes the cyber-threats against the future health care systems and the models that are used to conduct a threats analysis of e-health infrastructures and services. Section 5.4 deals with making and modelling of a threats analyses and the last section presents our conclusions, solution model and future work.

5.3 The research questions addressed in Chapter 5 are as follows

RQ 4. How can we verify that information from patient sensors and IoT devices goes to the appropriate data centres that are used only by authorised people?

> RQ 4.1. How can we verify e-health and other critical systems so that we can use them safely in the digital environment?
>
> RQ 4.2. How well do EU directives, national laws and recommendations guide our development and work to respond to patient information security, privacy and critical patient information?

5.4 Description of the future operating environment

The hospitals and healthcare centres are the key treatment points for examining and caring for the sick. In many situations, access to treatment takes time, possibly because of a shortage of healthcare personnel, but also because long geographical distances may impede medical examinations or access to treatment. As long distances also increase costs, it is not always possible to achieve a cost-effective solution with each treatment situation. People may have to travel long distances to a care point only to have their situation checked, which could have been done using a digital system. As a result, the

development of digital methods of treatment with sensors and IoT devices is strongly required to improve patient care and to examine patients' conditions remotely and in real time. Figure 58 illustrates the future healthcare operation environments.

To improve health care systems, new digital hospitals have been introduced which are more cost-effective than previous traditional hospitals, that are geared towards better treatment accuracy and performance in treatment processes and are more effective in diagnosing diseases. The digital hospital environment utilises the digital Hospital Information Systems which are the one main systems in this operation (Figure 58). In the future, the patient will be able to have several digital sensors and IoT devices attached to them to collect their health-related bio-signals, which are sent through the patient's smart device to the hospital information systems for analysis and follow-up (Figure 59).

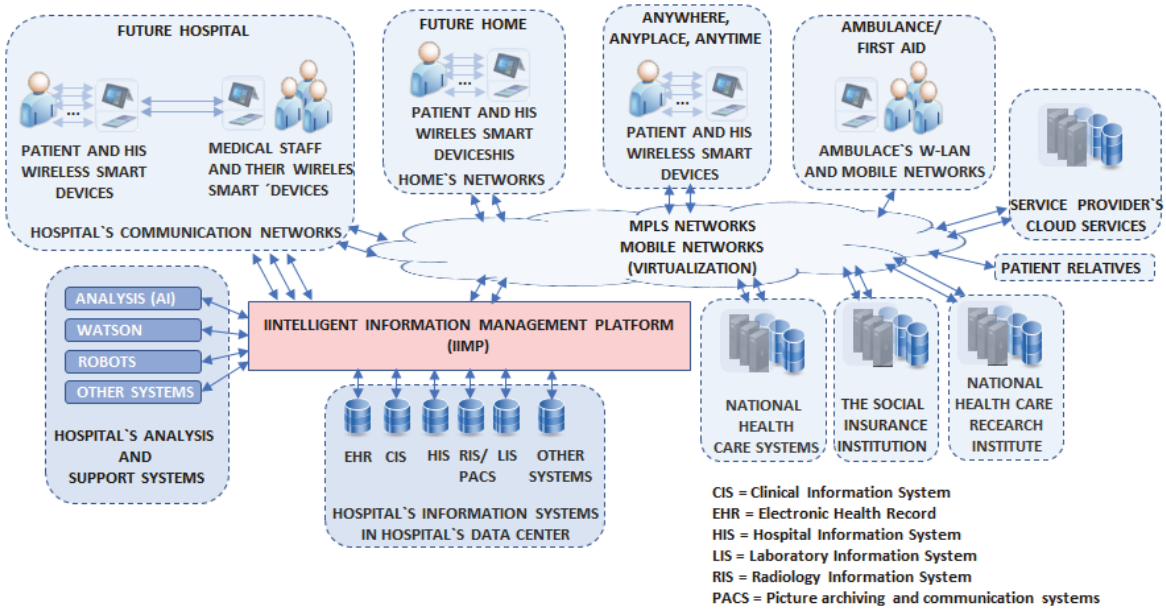


FIGURE 58. E-health or M-health operating environment, top level architecture, based on M-files ideas (M-Files).

The taxonomy of E-health or M-health systems can be described as data streams and processes, where patient information is transmitted via communications systems and stored in a hospital medical information system for data analysis and conclusions (Prasad, 2016).

Patients e-health or m-health sensors and hospital healthcare system taxonomy comprises the following categories: health and wellness monitoring, diagnostic sensors, prognostic and treatment sensors and assistive sensors. Each category is divided into sub-categories, which are further subdivided. Intelligent Information Management Platform (IIMP; Figure 58) systems are needed to monitor the flow of information obtained from patients' IoT devices and sensors. it also enables health care staff to analyse the information quickly, which ensures that care staff can find out information about patients for analysis in critical situations. This type of system can also help health care staff to notice possible anomalies or changes in data, or if someone has attempted to penetrate or use the data in an undesirable way.

The hospital has its own LAN and wireless network (W-LAN) through which medical records are sent to databases in the hospital's data centre. The medical data in the

hospital databases can be monitored by doctors and medical staff to make the necessary patient care decisions and management measures. The sensors and IoT devices belonging to the infrastructure's automation systems are also connected to the hospital's LANs and to all the hospital's internal communications systems, but this comes with risks.

This setup means that all smart IoT devices, sensors and terminals would use the same network systems and connect to the hospital's data centre. The hospital's networks and data centres have connections to the internet and to various external information systems such as National Health Care systems and National Social Insurance systems (Figure 58), which are the main systems concerning healthcare information and people healthcare insurance systems.

Communication between the patient's smart device and IoT devices and the sensors attached to them is done through fixed wired connections or wireless connections, including different wireless technical solutions such as different versions of Bluetooth: ZigBee, W-LAN, RFID and WiGig, (Figure 58). These technologies allow for connection distances ranging from 1 to 100 metres. When the hospital has a wide range of sensors and real estate automation systems that operate in the same frequency bands and when same frequency bands can also be used in hospital staff devices, the emergence of incidents is possible in the form of mutual interference. The new public buildings that are being built under the EU directives can also prevent the operation of wireless communications due to the large damping of the walls and windows of the buildings, meaning that mobile networks cannot work properly indoors (EU-NIS). The patient's home may also contain many sensors and IoT devices that use the same connections as the patient's smart device, which may cause interference (Figure 59).

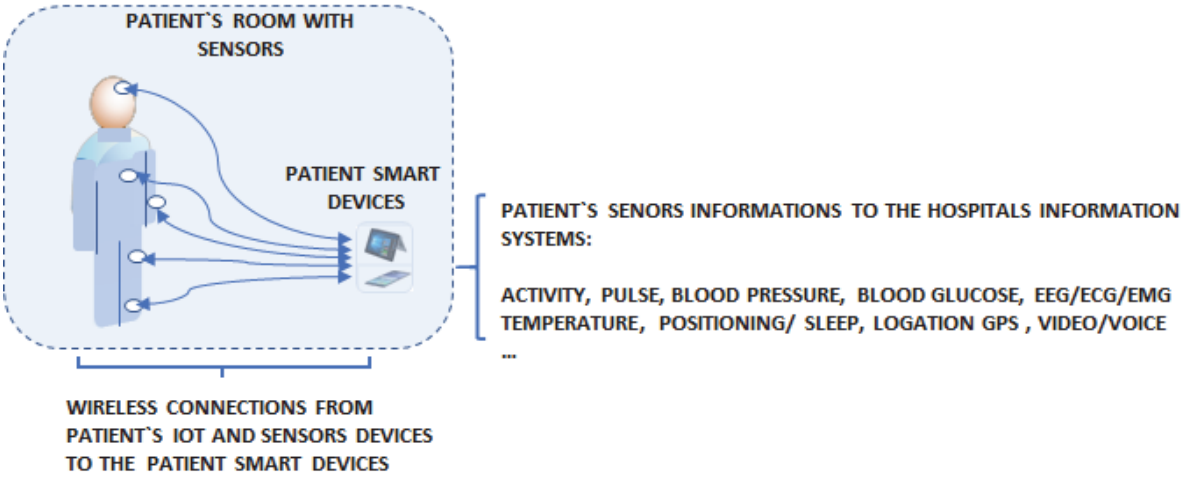


FIGURE 59. Patient's IoT and sensor devices connections.

One important factor in the treatment of patients in the digital environment (Figures 58 and 59) is to ensure the proper functioning of communications. When we talk about the human spirit and related issues, it is also necessary to take into account that digital devices do not operate without electricity. It is essential to ensure that patients have communications systems that work in rural areas where the supply of electricity may be cut-off for hours or even several days due to storms or snow disasters so that the doctor continues to receive information about the patient.

Doctors and/or medical staff should also be able to monitor the patient's condition at home in a real-time situation so that the necessary steps can be taken in time to guide the patient to necessary measures (Figure 60). Figure 60 shows the flow of patient information from their smart device to the hospital system from which the medical staff receives the information and sends feedback to the patient's smart device. In this way, the exchange of information between the patient and the care staff is carried out at a general level, whether in the patient's hospital, at home or outdoors. Table 14 shows the bandwidth needs of the patient's sensors in the communications networks and the transfer rate the data are transferred via telecom networks. Table 14 also shows the delay values that must be reached through communication connections. The values in Table 14 are obtained from the research results but are not the actual requirements or recommendations of our nursing systems.

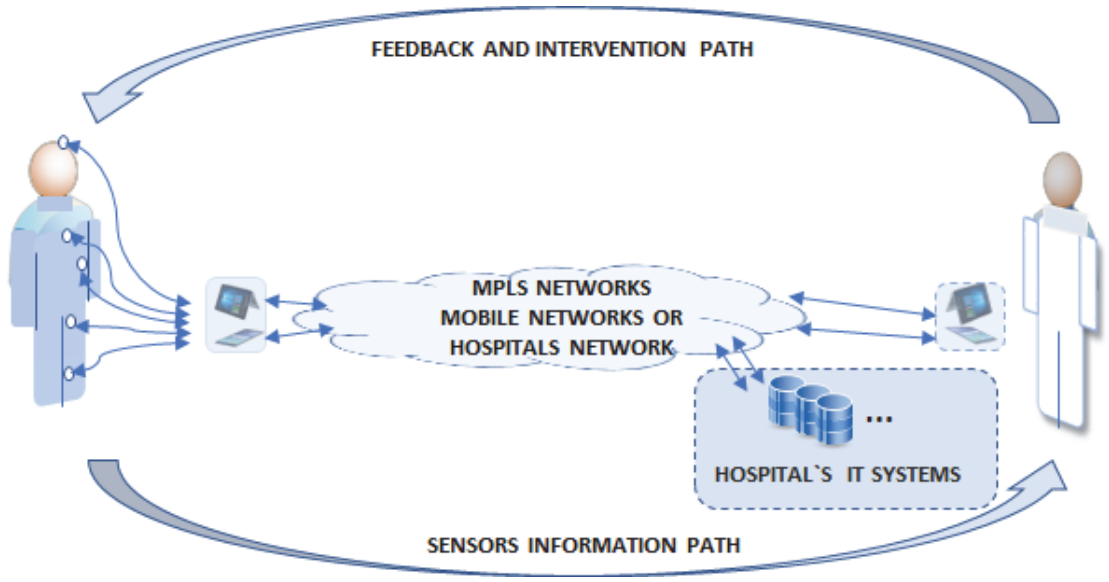


FIGURE 60. A general wireless and fixed m-health monitoring system.

TABLE 14. Data Rates and Bandwidth of Key Biomedical Wireless Monitoring (Prasad, 2016).

Physiological/Biomedical Parameter	Bandwidth	Rate Latency/Data
ECG (12 leads)	0.1 – 1 kHz	~144 Kbits/<200 ms
EEG (12 leads)	0.1 – 0.2 kHz	~40 Kbits/<300 ms
EMG	0 – 10 kHz	~350 Kbits/<200 ms
Body temperature	0 – 1 kHz	~0.1 kHz
Medical imaging and video streaming data	-	~ > 10 Mbps/ <100 ms
Speech and voice	-	~50–100 Mbitps/ <10 ms
Accelerometer and motion sensing	0 – 0.5 kHz	~30 Kbitps
Blood glucose monitoring	0 – 40 kHz	~1.5 Kbits
Blood pressure	0 – 1 kHz	~15 Hz

5.5 Cyber threats against future health care systems

As Figure 58 showed, the future health care information systems is an extensive and complex package that has a range of cooperation requirements, example between doctors and nurse, for the patient's wellbeing. The operating environment incorporates many wireless technologies, and the operating systems do not form a closed set without connections to the outside world. In addition, the health registers (EHR, HIS, LIS) include the personal data of all citizens and information about their illnesses. These systems are linked to external systems and allow people to send information to those systems, which then raises the interest of hackers and cyber attackers to penetrate the health systems because there is a chance of an economic benefit. Cyber attackers can also use the system vulnerabilities to harm selected people (EU-Energy Efficiency, 2012) (Brandon, 2017).

The following are security threats in wireless health networks:

- monitoring and eavesdropping of patients' vital signs
- threats to information during transmission
- routing threats in networks
- location threats and activity tracking
- denial of service (DoS) threats
- interfering with or inhibiting the radio communication of IoT devices and sensors
- using vulnerabilities to obtain access to the health care services
- attacking the hospital healthcare information systems
- disrupting or impeding the entire hospital's wireless communication and preventing the use of the hospital's daily activities.

If attackers know a patient location, they can follow the patient's route to where they live and determine what route or bus or train they use or the kind of car they use. An attacker could also find vulnerabilities in a patient's smart device and cause an accident while they are driving. After the accident, the accident investigators would wrongly assume that the accident occurred because the patient had a disease-related attack. This sort of attack is more likely to happen to people in prominent positions. An alternative goal of an attacker could be to use the smart devices to get inside the systems from which people receive grants (Figure 61), which contain billions of euros. When a cyber attacker attacks the health and hospital systems, they can quickly paralyse the entire society and make people worry for their future (Aurore LE BRIS, 2016).

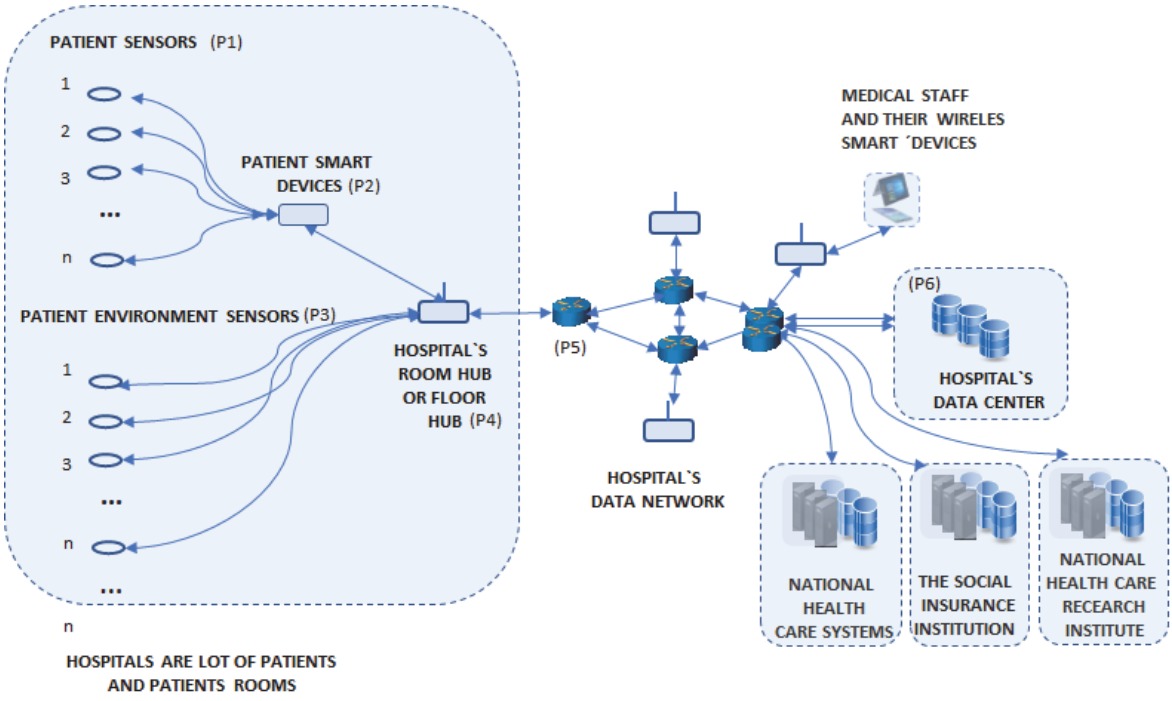


FIGURE 61. A general wireless and fixed m-health monitoring system with environment sensors in hospitals.

5.6 The making and modelling of a threat analyses

Figure 58 shows that healthcare systems are extremely complex and have many interfaces that connect systems and devices to wireless or fixed networks. In addition, there are several service providers, admins and stakeholders working on the same networks and information systems. In the operating limits of the responsible actors must be able to define and instruct the functions so that interoperability is ensured between the operators and those using the services. To conduct cyber-threat assessments and analyses, we must first work with architectural descriptions of the operating environments of the hospital, home and outside the home with equipment and operating processes. To prevent or even reduce the risks described in Sections 5.3. and 5.4., all parts of the healthcare systems should be segmented into their functional parts and a distinction should be made between them using a safety mechanism, which is a certain type of GW solution. These segments can then be examined based on use cases. We must also look carefully at the attackers and their capabilities as well as their motivations to disrupt the health care systems and organisations (Table 13).

Thereafter, data streams can be defined from the bio-signals produced by the patient's sensors to the servers. These data streams can be used to identify the devices and systems associated with each use case situation and to view the related dependencies and vulnerabilities. A risk analysis can be done based on dependencies and vulnerabilities, making it possible to determine the probabilities of cyber threats. The detected dependencies, risks and vulnerabilities can be exported to a table where they are easily extracted for mathematical processing. Dependencies, risks and vulnerabilities can be given as an estimate of the probability of realisation that can be utilised in mathematical review. We can use attack tree models to count the probabilities

of cyber threats. In addition, preliminary analyses of the tabular form can be used, which have already defined based on a sensitivity analysis and a preliminary assessment of each threat. Mathematical processing clarifies the threats to systems and gives a better picture of the threats. Mathematical processing also makes it possible to compare the cases in parallel and to make decisions based on the results; this is worth doing for the sake of target of attacks and to see the effects of the measures in the test.

TABLE 15. Capabilities and Motivations for Disrupting Health Care Systems and Organisations

	Patient Health		Patient/Hospital Records		National Health Care Systems	
Adversaries/ Attackers	**Targeted (Specific Victims)**	**Untargeted (Not Specified)**	**Targeted (Specific Victims)**	**Untargeted (Not Specified)**	**Targeted (Specific Victims)**	**Untargeted (Not Specified)**
Individuals/ Small Group				**Yes**		
Political Group/ Hacktivists			**Yes**			
Organised Crime	**Yes**		**Yes**	**Yes**	**Yes**	**Yes**
Terrorism/ Terrorist org.	**Yes**	**Yes**		**Yes**	**Yes**	**Yes**
Cyber Attackers			**Yes**	**Yes**	**Yes**	**Yes**
Nations, States	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

Figure 59 shows the various use cases for E-health or M-health situations. From these cases, we can review the service chains and look for dependencies, risks and vulnerabilities, giving them a probability values. Table 16 contains the values which can be used to calculate the probabilities for each case. Figure 61 represents the use case in which the patient is hospital. Figure 61 shows that several IoT devices and sensors are connected to the patient's smart device and that the device is connected to a room or floor access point (HUB). The same base station is also connected to various heating, ventilation, air conditioning and cooling systems (HVAC) systems. Manipulating all these systems can allow an attacker to access and exploit sensitive data stored in hospital data centres (ABC News, Jun 29, 2017).

Conducting a threats analysis of the whole future hospital system, or of just an entity comprising the service sectors as part of the future intelligent healthcare systems, is a challenging task. Therefore, a threats analysis is made based on Figure 61. The communications systems consists of access networks, a patient's room with IoT devices (P1 1…n), a patient's smart device (P2), a room HUB with HVAC systems (P3), core networks (P4) and data centre networks (P5). The threats analysis of the patient's access network shown in Figure 61 is currently subject to major changes because it involves large quantities of different sensors and IoT devices. The starting point for the analysis is a smartphone interface, with the IoT devices connected to it and the connection of the smartphone to the patient's room HUB system and to the hospital core router. The core

router may be virtualised and include some services in their hospital system's own slices. The HUB system may also include FW functions.

Section 5.4. presents examples of how attackers attempt to use vulnerabilities and other mechanisms to gain access to systems and compromise a target device. In these calculations, the values for these vulnerabilities are obtained from the analysis. The events must be independent; However, if situation is not in this way, we will need to make such small entities in order to gain independent situations over the various functions in our system. The review can be further deepened by examining and analysing the vulnerabilities of different OSI layers.

TABLE 16. Threats and Risks Table

Ref ID	Org	Func-tions	Cate-gory	Threat	Threat/ Risk	Existing Control	Threat / risk level			Accept /reduce	Recom-mented control	Residual threat/ Risk			Check Point
							L	C	R			L	C	R	
1 / AH	MC	Iden-tify	Access	Foot-printing	Target Access	IDS / IPS	3	3	8	Reduce	EU- dir.	2	2	3	1.1. 2020

L = Likelihood, C = Consequence, R = Risk

For probabilistic analysis, a defender needs to estimate the probability of attack success for each node in Figure 61, in the ADT. For the purposes of the review, we define the used notations.

TABLE 17. Meaning of Notations

ACTION	EXAMPLES	NOTATION
ATTACK	SNIFFING, ENUMERATION, SCANNING, …,	A
DETECTION	PORT SCAN, INFORMATION SCAN, …,	D
COUNTERMEASURE	ANALYSING OF VULNERABILITIES AND TO REPAIRING, AFEGUARDS PUT IN PLACE, …,	M

The probabilistic success of attacks ($P(t)$):

$$P1_{1\ldots n}(t) = p1_{A1\ldots n}(t)\,(1 - p_{D1\ldots n}(t)), \quad (1)$$

to n Patient's IoT devices,

$$P2_1(t) = P1_1(t)[(p2_{A2}(t)\,(1 - p2_{D2}(t)], \quad (2)$$

through an IoT device to a smart phone,

$$P2_{1\ldots n}(t) = [(p2_1(t)) + (p2_2(t)) + \ldots + (p2_n(t))], \quad (3)$$

because different IoT devices connect to smart phones at different times,

$$P3_{s1\ \ldots n}(t) = P_{3As1}(t)\ (1 - P_{3ds1}(t)),\ \ldots, \quad (4)$$

to a room connected with sensors 1 … n,

$$P4(t) = p_{4A1}(t)\ (1 - p_{4D1}(t))\ (1 - p_{4M}t), \quad (5)$$

to a HUB $_{(room)}$ with attackers, defence and countermeasures,

$$P4_s(t) = [(p_{3S1}(t))\ (p_{3s2}(t))\ \ldots\ (p_{3sn}(t))]\ [p_{4A}(t)\ (1 - p_{4D}(t))\ (1 - p_{4M}(t)], \quad (6)$$

to room sensors connected to the HUB $_{(room)}$,

$$P5(t) = p_{5A1}(t)\ (1 - 5_{4D1}(t))\ (1 - p_{5M}t), \quad (7)$$

to the router $_{(hospital)}$ with attackers, defence and countermeasures

$$P_r(t) = [p_{5A1}(t)\ (1 - 5_{4D1}(t))\ (1 - p_{5M}t)]\ (P4_s(t)), \quad (8)$$

to the router $_{(hospital)}$ and HUB $_{(room)}$ connected,

$$P6_{dc}(t) = P_{r1}(t)P_{r2}(t)\ \ldots\ P_{rn}(t), \quad (9)$$

and to the hospital's data centre router and all hospital routers $_{(hospital)}$ connected together.

The results obtained are exported to the Threats and Risks Table (Table 16), which contains the entities, the activity and category to be considered, and the related threats/risks and controls. Table 16 shows the current probability, the resulting consequences and the current risks. In the future risks possibilities are evaluated with how the risks is addressed, what are the recommended controls and what are the remedies, with its responsible persons (including organisations). Finally, the equivalent values and checkpoints after the remedies are estimated. The table can be used separately for cyber threats and risks and columns can be added as needed depending on the issues and related contexts being assessed.

5.7 Conclusions and summary of results

A modern hospital has hundreds – even thousands – of workers using laptops, computers, smartphones and other smart devices that are vulnerable to security breaches, data thefts and ransomware attacks. Hospitals keep medical records, which are among the most sensitive data about people. And many hospital's electronic systems help keep patients alive by monitoring vital signs, administering medications, and even breathing and pumping blood for those in the most critical conditions.

We can say, that anything that is plugged in, whether it has a Wi-Fi connection or not, is vulnerable to being hacked, and many medical devices, such as pacemakers and ventilators, are connected to the internet for the benefit of the patients. For example,

pacemakers can connect to a device at home that monitors the rhythms of the heart and sends the information to doctors. Hospitals also have a wide range of support systems and different analytical systems, such as Watson or other analytics systems. In addition, hospitals are increasingly using robots, for example, to dispense medicines. It is important to protect these systems from external security breaches, data thefts, ransomware attacks, security attacks and even cyber-attacks.

Nowadays, IoT-products and sensors mainly use proprietary based standards and it is almost impossible to obtain real information about the way they behave when they are connected to the patients' smart device. Those devices in use are quite critical and give hackers and cyber attackers many possibilities to attack patients' e-health systems and the hospital healthcare systems.

When using many IoT and sensor devices in hospitals environments, which use the same frequencies, there may be a lot of interference between the devices; this is an area of future research. If we use 5G and other wireless technologies in the hospital environments, there will be a lot of different frequencies in use on the same floors and in the same buildings. The frequencies radiation limits must be defined for IoT and sensor devices so that they are safe for use by patients. Future research could thus measure and test the frequency disturbances in the hospital and patients' home environments to check whether any possible cases might affect the patients' treatment.

The use of AI needs to be investigated and tested for its ability to protect e-Health's IoT devices, sensors and other health systems so that we can better protect these devices against malicious software and cyber-attacks.

Because healthcare devices contain many vulnerabilities and security challenges, we need to develop effective architectures for healthcare equipment and systems so that patients and treatment staff can use them safely in the medical care environment (EU-GDPR, 2016) (EU-MDR, 2017)(Foster, 2013).

Energy efficiency is also an important research area to investigate in the health care environment and in relation to health care smart devices.

5.8 Our ongoing E-health research project

In our ongoing e-health research project called 'Intelligent Medical Devices', the author presented architecture descriptions of smart home architectures and smart hospital architectures, which include security architectures and the IoT devices and sensors in those future environments (Shishir Kumar Shandilya, Soon Ae Chun, Smita Shandilya, Edgar Weippl, 2018) (PI). In this architectural work, the author presented a system called 'IIMP', which can be used to monitor the patient's IoT devices and the sensors' flow of information to hospital healthcare systems to provide healthcare personnel with a rapid analysis of the information. `IIMP` also ensures that medical staff can find information about patients even in critical situations. This type of system can also help to find possible anomalies or data changes or identify if someone has attempted to penetrate or use data in a way that is undesirable (Dongfeng Fang, 12-2017). The user can create specific action groups for this system, which can only be accessed through a license. There, the members of the user group can follow the progress and changes to some situations and to related data resources and reports in real time. In this arrangement, federations can be created between the different systems and create a log

of information. This IIMP platform can also be used in other areas of smart city systems like city offices information systems and follow information flows in the really complex environments of smart society systems. Basic idea is quite near of M-Files architecture and system (M-Files) (PI).

As the technical manager and architect, and as the security network architect for more than 10 years, the author worked on the 'security authorities project' and was also involved in the development of national safety requirements (VAHTI and KATAKRI), these included the audit requirements of different equipment that we used in our networks. Based on these VAHTI and KATAKRI requirements, it is possible to perform an analysis and to determine whether a system or device can be used in real environments.

IoT devices and sensors have been tested with platforms on smart devices but the security issues have not yet been tested. The research project 'Smart medical devices' will be launched in the beginning 2020, which takes into account the findings of several previous materials and research studies (EU-GDPR, 2016) (EU-NIS, 2016) (Istepanian, Woodward, 2017).

Our goals are as follows:

1. Develop practices and guidelines for the safe use of medical devices.
2. Develop specific usability standards for medical devices aimed at the safe use of equipment.
3. Create addiction, risk and cyber-threat analysis for patients connected IoT devices.
4. Create an addiction, risks and cyber threats analysis for the service chain through which bio signals from IoT devices pass between the patient's home and the hospital. The service chain is made up of the patient's IoT device and the hospital or service provider's server regardless of time and place.
    a. The study seeks secure solutions for implementing IoT devices and connecting them to various smart terminals.
    b. Solutions seek to find energy-efficient and long-term solutions, such as zero-energy technologies.
    c. The security and cyber threats to hospitals and home environments are being researched and analysed, as well as interference from building automation and IoT flat panel sensors and IoT panels to make the necessary changes to technical solutions. For example, forensic testing can ensure that the patient's bio-signals are from the right patient and do not change when they go to the data centre and the hospital's patient information system.
5. Determine how the infrastructure secures the connection of the terminal so that only the specified devices can communicate on the data network.
6. Examine the power consumption of IoT devices (e.g. battery/battery protection).
7. Explore how medical devices and wellbeing support the patient's wellbeing and whether they can be used in disease prevention.

Author's works in the 'Intelligent Medical Devices' project:

The author has performed a risks and cyber threats analysis for the service chain through which bio signals from IoT devices pass between the patient's home and the hospital. I created a table of the capabilities and motivations for disrupting healthcare systems and organisations (Table 15; PIV). In future projects, I will continue to analyse the risks and cyber security issues concerning future hospital and home environments.

5.9 Answer to the research questions, conclusion and future work

Answer to the research questions:

RQ 4: Figure 58 shows the process of Intelligent Information Management for hospital environments and it gives possibilities of how to follow and verify that patient sensor and IoT -device data are going to the right place and are accessible only by authorised healthcare individuals.

> RQ 4.1: Chapter 6 presented a new type of device which protects communications path so that we can use critical systems information safely in these digital environments.

> RQ 4.2: The author and his colleagues are working on a research project to clarify the EU directives, national laws and recommendations for these hospital systems to ensure the patient's information security, privacy and critical patient information are protected and used in the right way.

Conclusion

The future complex environments present many challenges because the standards are not yet set at the international level [94]. IoT products and sensors are mainly used at proprietary-based standards and getting them work at the same platforms in the smart devices will be a really big challenge (Shishir Kumar Shandilya, Soon Ae Chun, Smita Shandilya, Edgar Weippl, 2018) (Istepanian, Woodward, 2017) (STAT, by ASSOCIATED PRESS, 2018). We have divided our project into seven smaller parts so that it is easier management those issues.

Future work

A modern hospital has hundreds – even thousands – of workers using laptops, computers, smartphones and other smart devices that are vulnerable to security breaches, data theft and ransomware attacks. Hospitals keep medical records, which are among the most sensitive data about people. And many hospital's electronic systems and devices help keep patients alive, monitor vital signs, administer medications, and even breathe and pump blood for those in the most critical conditions.

We can say that anything that is plugged in, whether it has a Wi-Fi connection or not, can be vulnerable to hacking, and many medical devices, such as pacemakers and ventilators, are connected to the internet for the benefit of the patients. Pacemakers can

connect with a device at home that monitors the rhythms of the heart and sends the information to doctors.

Hospitals also have a wide range of support systems and different analytical systems, such as Watson or other analytics systems. In addition, hospitals are increasingly using robots, for example, to dispense medicines. It is therefore important to protect these systems from external security breaches, data thefts, ransomware attacks, various security attacks and cyber-attacks.

Nowadays, IoT-products and sensors mainly use proprietary based standards and it is almost impossible to obtain real-time information about patients' behaviour when we connect them to the patients' smart device. The devices currently in use are quite critical because there is a lot of vulnerabilities in and this give hackers and cyber attackers many possibilities to attack patients' E-health systems and hospital healthcare systems.

The use of many IoT and sensor devices in hospital environments which use the same frequencies could create considerable interference between the devices; thus, this is an area of future research. Additionally, if we use 5G and other wireless technologies in the hospital environments, there will be a lot of different frequencies in use on the same floors and in the same buildings. Radiation frequency limits must be set for IoT and sensor devices to ensure patient safety. Therefore, future research will measure and test for frequency disorders of the hospital and the patient's home environment to determine if potential interferences may affect patient care and there is same time measured also radiations values. In future work should also investigate the use of AI to protect e-health's IoT devices, sensors and other health systems so that we can better protect these devices against malicious software and cyber-attacks.

Because existing healthcare devices contain many vulnerabilities and security challenges, we need to develop good architectures for the healthcare equipment and systems and apply the legal requirements so that patients and the treatment staff can use them safely in this medical care environment (EU-MDR, 2017) (EU-NIS, 2016).

Energy efficiency is also an important research area to investigate in the healthcare environment and in relation to the healthcare smart devices.

CHAPTER 6. SOLUTION MODEL FOR NEW TYPE SMART DEVICES AND NETWORK, SYSTEMS AND DEVICE, PVI AND PVII.

6.1 Introduction

In practice, there are many domains where reliable communication capabilities are needed, mobile networks often do not work for one reason or another, and direct D2D communication between devices would work better. Such situations include emergency situations in the hospital, in the patients´ home and when patients are out of home. Patients´ smart devices may do not work well and also hospital medical devices may be not work well. These situations also need energy efficient solutions for devices such as 3GPP-5G, METIS 2020 are recommended in the 5G requirements. In practice, there have been many situations where communication with current technologies does not work well or does not work at all and messages between authorities and people do not work in the critical situations when needed, example in 0-energy buildings.

For example, every year in Finland, there are storms that cut off power lines and, as a result, base stations for mobile networks are left without electricity. After a few hours, the networks stop working meaning that the devices based on mobile technology also stop working. New buildings, particularly the so-called zero-energy houses attenuate the radio signal which are coming in and going out so that in these situations, devices based on wireless technology cannot be used properly. Firefighters face this challenge in many situations because smoke can interfere with audibility (this situation found during firefighting operations). As the rescue director must always be able to communicate with his men in real time, they require a cross devices direct function that enables D2D functionality, which is being introduced with 5G technology, but does not eliminate the need for power in different drives. Our patented device includes D2D functions.

In VIRVE terminals, D2D functionality already exists, but it only works between the terminals and cannot function with normal smartphones, which prevents collaborative activity in critical situations. Many times, the situation is also extremely

critical in areas where base station coverages are inadequate, and the slightest disruption can lead to disaster.

Currently, considerable research is focusing on the development of autonomous car and robot traffic. The communications needed there must work reliably with minimum delays at every moment because the response times are short, e.g. motorway and city driving. However, for transmission via base stations mounted on the roadside, the transmission of signals between vehicles is relatively slow. In this situation, vehicle-to-vehicle direct traffic is required, for example, to prevent collisions. In addition, if roadside base stations lack electricity as a result of a storm or other disasters, the automatic traffic control function will be almost completely prevented. In those situations, the traffic can also be disrupted by a large truck travelling on a highway between base station and a smaller car, temporarily preventing radio signals from passing.

One application area that can work with this arrangement in, for example, wilderness areas or in the Arctic, where there are no base station networks, is drone networks as these can be used in various search and rescue missions.

In practice, this patented concept allows the devices and system to operate independently of other networks at anytime and anywhere without the need for other mobile network solutions.

The tsunami disaster in Aceh was one example where telecommunication arrangements had to be put in place to help people quickly. The author prepared a concept for a tsunami rescue operation based on a movable network concept (which the author was also developing). Satellite telephones were used in the initial phase, but local solutions required even more flexible solutions.

This patent concept presented above is an effective solution because it does not require other mobile networks to operate around; It also provides interfaces to existing mobile networks that allow communication with local authorities, example there in the tsunami disaster in Aceh. Similar actions could be taken in hurricanes and other natural disasters, where the entire region has been destroyed, energy is inaccessible and/or no telecommunication systems are in place. This proposed solution could also complement satellite-based solutions.

All of the abovementioned environments require a mobile network-independent solution that can be deployed quickly in the area and can connect people from different countries for rescue operations with local authorities for successful leadership and rescue efforts.

The devices of this patent type can be operated using new protocol technology that has been researched and tested in a PoC test.

Because of the many security challenges, in security solutions and the privacy and cyber security issues in current healthcare systems, this new type of smart device will be tested in those environments, which uses a new type of security solutions. In the patient's hospital room, the patient's and care staff's intelligent devices work together (D2D) and exchange information directly in real time without the need for another network. Smart devices can work together forming their own network, device can go outside out of network, and come back network again seamlessly without any disturb. The device prototype, which was tested in the laboratory and in the field between 2015 and 2017, was found to work effectively. The device security system prevents

unauthorised persons accessing the device and the data transmission and the services provided, regardless of whether the patient is traveling or is located at home or elsewhere. The new systems must meet the requirements of the EU-GDPR and EU-MDR directives. The security issues of IoT devices and sensors with platforms on smart devices have not yet been tested (IEEE-11073-10419) (IEEE-11073-10417) (IEEE-802.11, WiFi) (Khajuria, Sorensen, Skouby, 2017). A research project on 'Smart medical devices' will be launched in the beginning of 2020, which takes into account EU-GDPR, -MDR and -NIS regulations.

We live in a digital world where people can be provided with increasingly effective treatment methods that allow them to live longer and better lives at home. By giving people IoT devices and sensors to carry, healthcare professionals can monitor patient's information while at hospitals but also in their homes.

Even though the digital world offers opportunities to improve the healthcare systems and improve the analysis of diseases, many challenges remain because individual devices and systems may not work well together. Almost every manufacturer has their own technical solutions that work only in certain environments.

Healthcare systems require high levels of coherence and information solutions systems. The healthcare devices technique used is very variable and based on manufactures own standards. While international standards for healthcare systems and devices are evolving, they are not yet complete. In addition, there is a lack of technical and functional requirements for telemedicine systems and devices, and the requirements for the provision of secure data communication in remote health care are also lacking (Finland). Therefore, 'thousands of patients around the world have been injured by incorrect medical devices' (Huttunen, Halonen, Koskimäki, 2017) (Huttunen, Halonen, 2018).

These lack of health standards or deficiencies were one of the reasons why a new smart device should be made on the basis of an approved US patent (PeAN).

Another reason was that smart devices contain many vulnerabilities, so using them as a smart terminal for a healthcare patient is a risk leaving the health systems at risk of attacks (M-Files) (Ramjee Prasad, 2016). The third reason was that intelligent terminals are used everywhere in smart societies and in the smart cities of the future, and they are interlinked and interact with each other (D2D, V2X and M2M). The delays of communications protocols available today present challenges to real-time communications, which then pose challenges to the development of critical communication systems such as e-health systems. Communications delay is one critical requirement in 5G development and energy efficiency is other critical requirement in 5G development (Huttunen, Halonen, 2015) (5G-PPP) (Osborne, Devlin, Barr, 2018) (Khan, Javed, Abdullah, Nazim, Khan, 2017). One area of research for energy efficiency in the future is zero-energy communication between IoT devices, sensors for patients and health staff smart devices. This energy efficiency is also the reason for developing new smart device concepts. New secure intelligent devices are also needed in this area to allow people to communicate securely with each other.

6.2 Research questions

RQ 5. Is it possible to implement D2D communication systems, for example, in hospital environments without any other communication network?

> RQ 5.1. How can we implement a service network quickly and flexibly where it is needed without any other communication network?

6.3 Research: PoC (phase 1) of PeAN.

A PoC was developed to demonstrate the real-world potential of the PeAN technology (based on a US patent, PVI). The goal was to ensure interoperability with the current networks and to provide seamless movability when roaming between networks. This ability was demonstrated by maintaining an active video call while moving between locations, representing a typical everyday use.

The PoC consisted of two local wireless networks that could be used by a nearby PeAN device. The device had 4G mobile broadband connectivity when moving out of the range of a local PeAN network. The PeAN device preferred to use local connectivity over mobile broadband whenever possible. In the PoC, the transitions from one network to another were made in the 'worst possible manner' by cutting the connectivity of connected network interface whenever the signal level of the interface was below a pre-set threshold. This allowed the engineers to develop a solution where the availability and quality of the network connectivity was maintained free of errors, even in worst case scenarios.

The scope of the PoC was limited to finding and demonstrating a solution to manage de-centralised traffic patterns and routing of the traffic efficiently between peers (Figure 62 – 64). At this stage, the configuration of the local networks was done manually. It was found to be feasible to use arbitrary ad-hoc connectivity between the PeAN devices. Thus, we could focus on developing network-formation solutions in the next stage of development. The test used a new type of protocol.

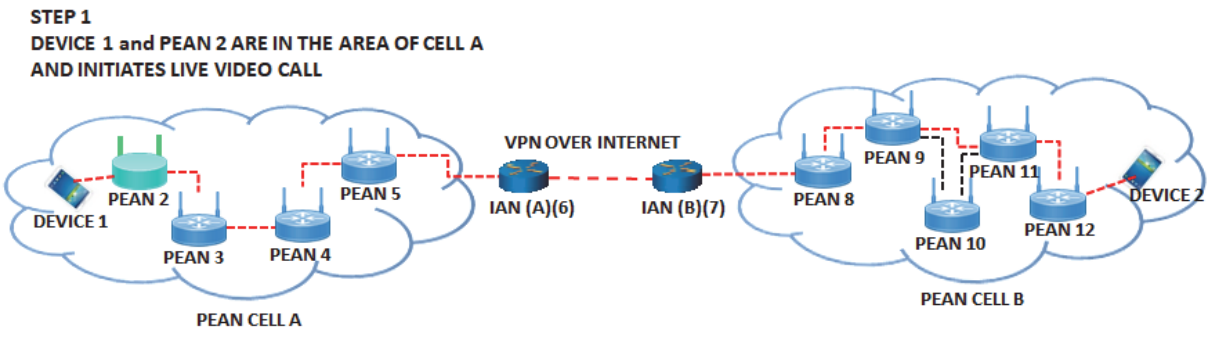


FIGURE 62. The PoC, Device 1 and PEAN 2 are in the area of Cell A.

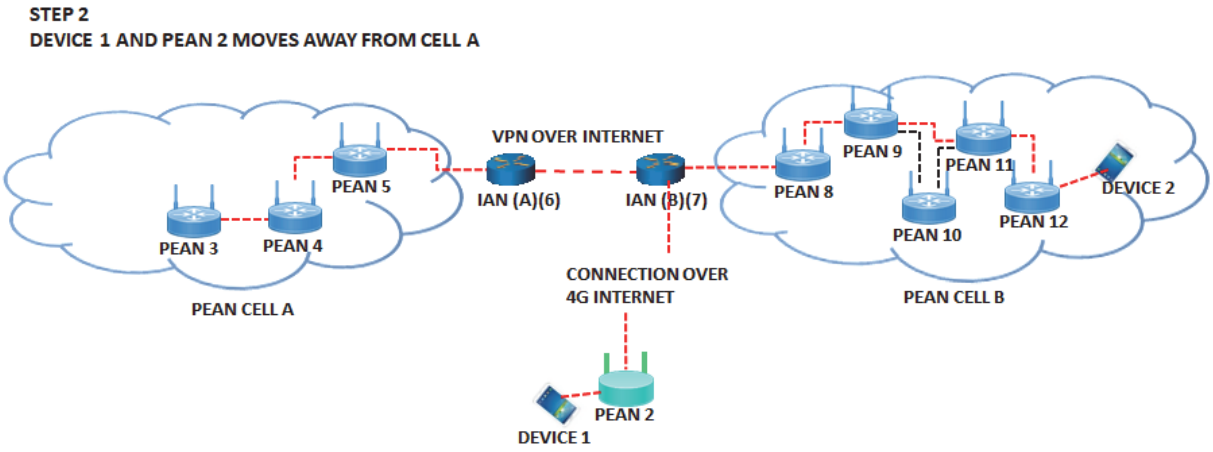


FIGURE 63. Device 1 and PEAN 2 are moving away from Cell A and are outside of the PEANs formed network.

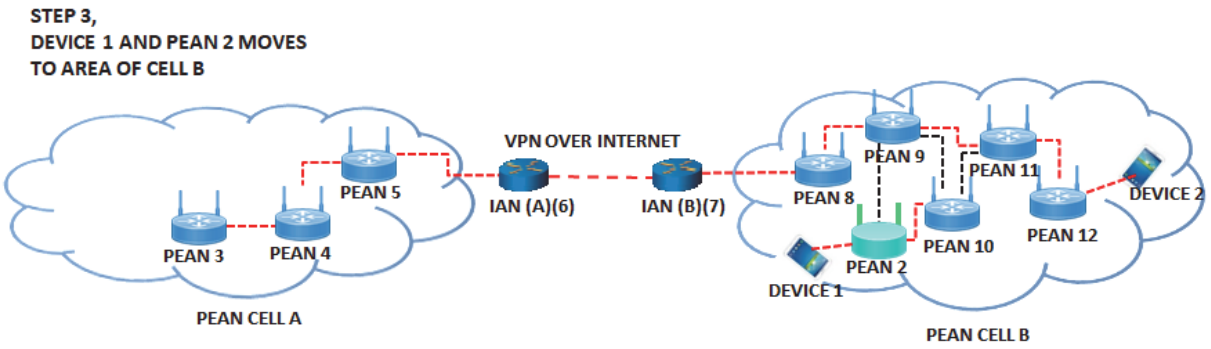


FIGURE 64. Device 1 and PEAN 2 move to the area of Cell B.

6.4 Invention claims

This section presents the invention claims (patent definitions = claims) which are used in the tests for requirements and definitions (PVI).

This new mobile smart device is adapted to function with several radio systems for sending, receiving and handling data in a telecommunications network including access network systems. It works like a smart base station with all functions needed to control the channels, services and surveillance services and for profiling users based on their user profile.

This device provides secure connections, fast authentications and/or authorisation services and enables corresponding services to a mobile user. Network control services and protocol modification and adaption services are also provided. The functions described above are in one device called an intelligent base station. A surveillance service controls and surveys the capacity used by the user.

The device is configured so that it can disconnect from an original network and connect and operate as one device forming its own mobile network with other devices in a one MESH-type network. The device can re-join the original network again and form an autonomic entity with the network. Inside that system are load and traffic control services so that the systems adapt to different loading situations.

The device is a transmitting and switching service for both data and speech. The communication in this intelligent mobile space station used may include pictures, moving pictures, speech, text, or a combination of these. As shown in Figures 62 - 64, the devices can form a mesh-type network with all the needed control functions to work with other devices without any other mobile networks. However, these devices can also use every available mobile network if needed and if there are acceptance to use them and they uses accepted SIM-card there.

This wireless communication network comprises at least two directional antennas from different directions, forming a complex, partly overlapping coverage area, whereby the user terminal receives contact to the service equally. Therefore, the user terminal gets a contact to the service simultaneously through both directional antennas and at least one is connected to the base station.

This also means that there are two different coverage areas, which gives possibilities to connect the user devices to two different base stations to get the best quality of services. If the base station forms a multidimensional grid structure, this concept gives possibilities to get the best quality of services in, for example, big buildings, hospitals and free time areas, and the user can use the best quality multiservice networks services as needed. This setup is important for e-health systems when patients are moving outside of hospitals or their homes.

6.5 5G requirements

An overview of future mobile communications

When considering the technical solutions and requirements in the design of future wireless communication networks and systems, we need to address their primary performance. One of the key features of this whole society is the provision of digital services to all citizens at anytime, anywhere and in real time. If the services do not work, at least some of society's activities are disrupted, which in turn affects the daily activities of many citizens. These services need reliable and secure communication systems, data centre systems and information systems.

When a society's services are provided through digital environments and are thus accessible to all those who need them at anytime and anywhere, the services must adapt to future changes in society. The EU has thus become involved in the development of the services needed for future society by supporting research and development projects. Next, in Figures 65 and 66, we look at the objectives and use cases for future communications networks and services, the different scenarios that will enable various future service environments to set in different use cases and their technical solutions (5G-PPP- White paper on 5G and e-Health, 2015) (5G-PPP- White paper on 5G and energy, 2015) (5G-PPP- White paper, view of 5G architecture, 2016) (Teec, 5G Mobile, 2017).

We also need to consider key technical issues in future service environments so that we can consider the security and cyber threats impacting them. In the future, social development will lead to major changes in the way mobile and wireless communication systems are used. As a result, an EU co-financed METIS project was set up in 2012 with the main objective of creating a basis for the development and testing of mobile networks and access networks from the year 2020 onwards. To start developing these mobile networks (5G), based on different use cases for the future, we must first define general scenarios and solutions based on the key features of the current mobile networks, identify the challenges we face and the services we want to improve, and determine how future systems will be able to meet their users' service requirements (Figure 65).

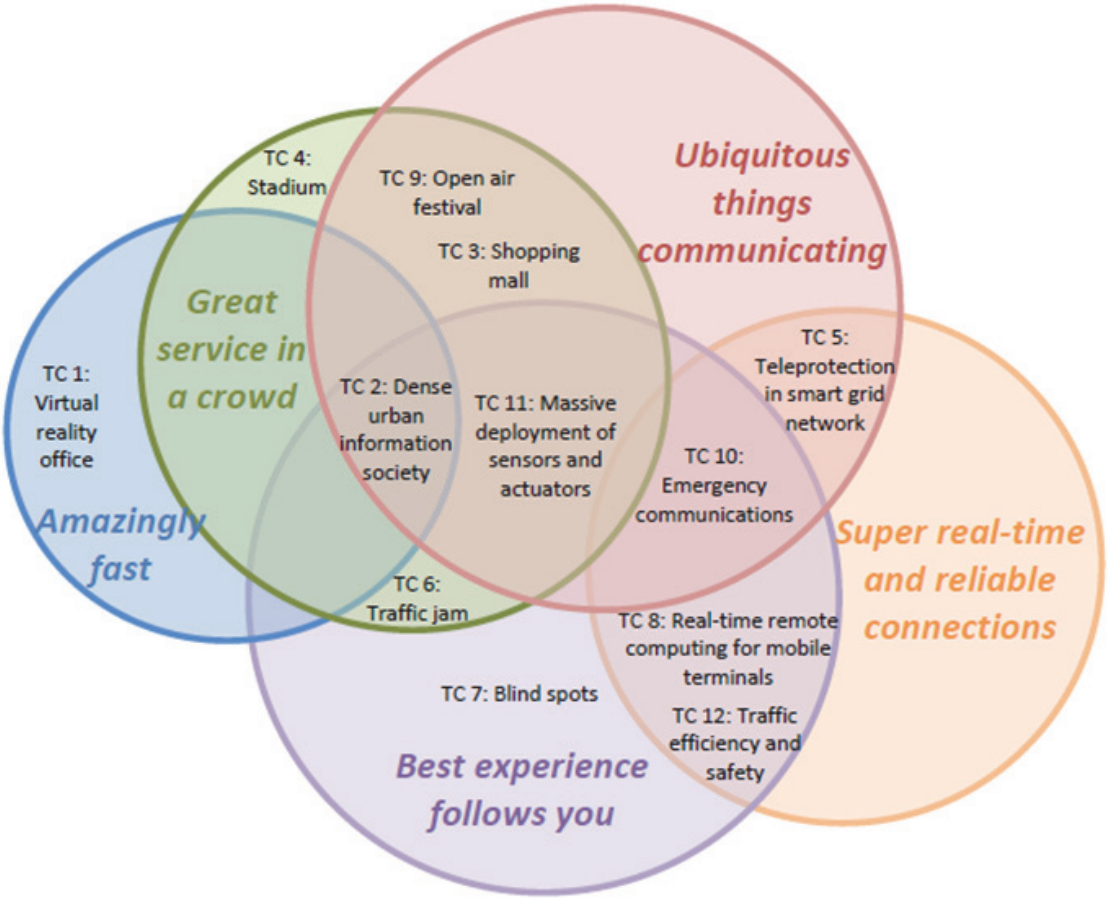


FIGURE 65. Mapping of the five scenarios and the 12 test cases (3GPP-5G) (5G Norma) (METIS 2020).

The specific characteristics of each scenario and each test case should include the key assumptions regarding the requirements and key performance indicators. To avoid constraining the potential solutions, the requirements are specified from an end-user perspective (5G-PPP- White paper on 5G and e-Health, 2015) (5G-PPP- White paper on 5G and energy, 2015) (5G-PPP- White paper, view of 5G architecture, 2016) (Teec, 5G Mobile, 2017).

Figure 65 identifies five scenarios and challenges for future wireless (5G) communication systems, and from them, 12 concrete test cases are defined to reflect

these fundamental challenges. From 2020 onwards, it will be necessary to provide quite different types of requirements for wireless communications than we have today. These requirements go beyond the natural evolution of IMT-Advanced technologies, which show the need for a new mobile generation, with certain different features with respect to legacy technologies (METIS). As shown in Figure 66, the main scenarios are Massive IoT, Mission-critical controls, and Enhanced mobile broadband, as well as regional refinements for each scenario. This is the device manufacturer's view of the technical requirements for future mobile networks, based on the Figure 66 scenarios and the requirements of 3GPP-5G, 5G-Norma, METIS-I/METIS-II.

METIS has defined that the following main objectives for the different systems have to be

- significantly more efficient in terms of energy, cost and resource utilisation than the current systems;
- more versatile to support a significant diversity of requirements (e.g. payload size, availability, mobility, and Quality-of-Service (QoS)) and new scenario use cases; and
- provided with better scalability in terms of the number of connected devices, densely deployed access points, spectrum usage, energy and cost.

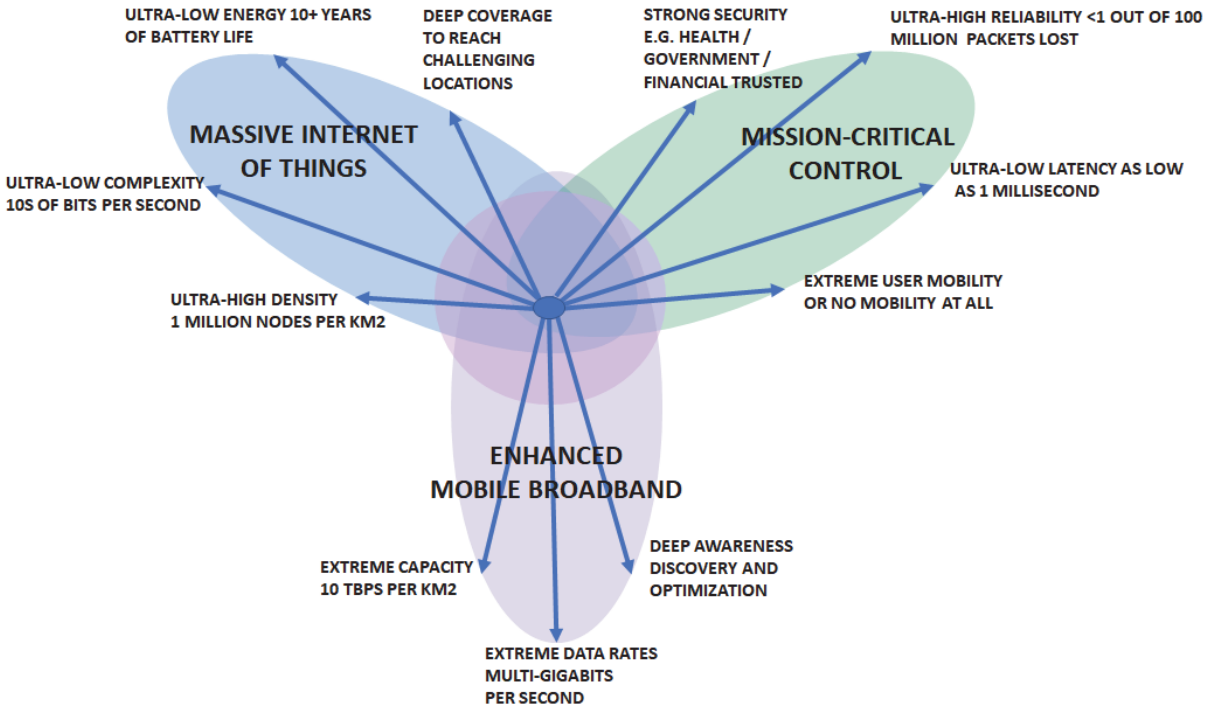


FIGURE 66. Future wireless systems using 5G will be scalable to an extreme variation of IoT requirements.

Figure 66 is based on Qualcom information.

The technical goals derived from the main objectives of 3GPP-5G, 5G-Norma, METIS-I/METIS-II.

- 1,000 times higher mobile data volume per area;
- 10 to 100 times higher typical user data rate;
- 10 to 100 times higher number of connected devices;
- 10 times longer battery life for low-power devices;
- 5 times reduced end-to-end (E2E) latency, reaching a target of 5 Ms for road safety applications.

The key challenge is to achieve the above goals with the same cost and energy consumption as the current networks. The technical targets derived from the main objectives of METIS 2020 show that limit values are reached and that existing systems do not scale with these requirements after 2020. We find that virtualisation has not been mentioned in the above requirements.

The author of this dissertation has also presented the effects of virtualisation on mobile networks (Appendix 1).

Regarding future communications networks and services, the technical objectives are derived from the main objectives of 5G, which have been adopted by 3GPP-5G, 5G-Norma and the METIS-I and -II groups for future 5G systems. These technical objectives mean also that we need to import the data centre's functionalities closer to the users, so that the services can be provided in accordance with these objectives. The reason for this is because the technical requirements, and especially the delay requirements for the signals to certain applications, are particularly challenging (< 5 ms delay); therefore, the functionality of the data centres must be bought closer to the users, and we need to consider the above requirements in future PeAN tests.

6.6 Answer to the research questions, conclusion and future work

Answers to the research questions

RQ 5: In the PoC test, we proved that our new device can implement a feasible D2D communication system. This concept can thus be used in hospital environments without any other mobile communication systems present.

RQ 5.1: Figures 62 - 64 show that we can implement a service network quickly and flexibly where needed.

Conclusion

The PoC has been completed and tested for the level of Layer 3 routing protocol functionality in an environment, where the network elements and the mobile network topology are changing. The test happened in real-time and continued at random. The PoC showed that, although elements of the network dynamically alter the location and

topology of the network changes, the protocol is capable of forming a continuous connection between the consumer terminals, such as a video call between mobile devices. When using the web, the connection route may vary randomly through several PeAN devices using the best route via a mobile network (4G or 5G) or via wired internet services.

Future work

Our future work will test PeAN in the e-health environments of hospitals and at individuals' homes. We have developed the research project 'Intelligent Medical Device' which uses real hospital and home environments and tests the effectiveness of the system when patients travel in any area. For those tests with e-health systems, we need to use 5G test networks and different types of access systems. We will use the claims of our two patents as a source of requirements and functionalities used in our earlier tests.

CHAPTER 7. SUMMARY OF DISSERTATION.

This dissertation examined future smart cities, smart societies and the Arctic region with services grouped into different segments, to better understand and address the needs of this rapidly changing operating environment. The key issues include ensuring cyber security, security of communications systems, energy efficiency and the provision of citizens' services at anytime and anywhere.

Although the infrastructures of the future smart city are divided into six segments with services and the environments' architecture works are described using the EA framework, it has not been easy to perform cyber security threats assessments and analyses in this rapidly changing and evolving entity.

In addition, digitalisation is constantly changing the operating environment in a fast and unprecedented way. Because the number of used devices, the amount of information in data centres and in our use, and our energy consumption are growing exponentially; cyber and security threats are also growing exponentially.

Countless IoT and sensor devices, wellness devices and computers can be connected to a user's mobile terminal using wireless technology. These devices operate in environments where a great deal of other wireless devices are used, such as home automation systems, home appliances and home security sensors. However, security for these devices may not be adequate or exist at all.

Energy efficiency and climate change are the most critical issues in our environments and must therefore be addressed in the systems we are using. In this dissertation, the author presented using virtualisation, profiling in the systems and zero-energy communications to decrease energy consumption and the amount of CO2 and greenhouse gases being emitted.

When we connect the continents to submarine optical cables, approximately 97% of intercontinental communications will pass through them, which will increase the interest of state actors in the use of submarine optical cable systems. State actors have the ability to tap (make a connection point) into underwater optical cables and collect and utilise the information contained therein. This development offers a huge variety of opportunities for state actors, cyber-attackers and hackers to attack our systems and collect information. They can also use satellite systems to send fake information and hide evidence of their presence. They can attack organisations from other continents or other countries and hide their footprint using various communications solutions.

Concluding remarks and future studies

To drive this development and its needs in the right direction, we need to perform a great deal of EA work; develop a common understanding of the structures of smart cities, smart societies and the Arctic region; ensure cooperation between different states, ministries and organisations; create cooperation between service providers in the smart cities, smart societies and the Arctic region; and develop an understanding of the factors that affect the future.

Considerable research and development are also needed in the fields of security and information security to provide a safe environment for services for users. This dissertation was used only public materials and information. Political and military issues are not addressed in this dissertation.

The following are the main results of this whole work:

- A high-level new description model that describes the infrastructures and services of smart cities. The model describes the various segments of smart cities with their services and the factors affecting them. The presented model makes it easier to group functions into segments and to define and develop smart city information architectures and their services, using the overall architecture framework. The model provides a clearer picture of service entities and facilitates the identification of dependencies and cyber threats in and across segments for analysis.
- A new model can be used to define cyber threats in different environments and calculate their probability of occurrence in different segments and intervals between segments.
- A new architecture and integration model for hospital systems, which allow for better control and monitoring of hospital data flows and the flow of bio-signals between the sensor and server of patient-used hospital equipment. This system will be better able to meet the requirements of the EU Data Protection Directives and thus protect hospital environments.
- Cyber-threat analyses have been also conducted for submarine optical cable systems and connections in the Arctic region and proposals are presented to protect their communications systems.
- Satellites and High Altitude Platform Services (HAPS) solutions are proposed for Arctic communications because they can provide services in areas without base station networks.
- The hybrid model of renewable energy system is presented with the energy savings it achieves. The model also provides a solution for the energy use of a small house in the Arctic. The model is also suitable for larger properties in urban and rural areas. The energy savings achieved using the hybrid model are presented step by step on a yearly basis.
- A new type of user mobile smart device based on two patents and tested in a proof-of-concept (PoC) test. The upcoming Intelligent Medical Devices project will test devices in the hospital environment and it start in early 2020. These new type of user mobile smart devices provide secure connections between the patient sensor and the hospital information system and thus protect the data. Development of the device takes into account the requirements of the 5G standard for mobile devices.

YHTEENVETO (SUMMARY IN FINNISH)

Tässä väitöskirjassa tutkittiin älykkäitä kaupunkeja ja älykkäitä yhteiskuntia sekä arktista aluetta. Palvelut on ryhmitelty eri segmentteihin, jotta ymmärrettäisiin paremmin näiden nopeasti muuttuvien toimintaympäristöjen tarpeet ja pystyttäisiin paremmin vastaamaan niiden palvelutarpeisiin. Keskeisiä aiheita ovat kyberturvallisuus, viestintäjärjestelmien turvallisuus, energiatehokkuus ja kansalaisten palvelujen tarjoaminen turvallisesti milloin tahansa ja missä tahansa.

Tulevaisuuden älykaupungin infrastruktuuri on jaettu palveluineen kuuteen segmenttiin. Niihin liittyvät arkkitehtuurityöt on kuvattu kokonaisarkkitehtuurimenetelmän (EA-menetelmä) avulla tarvittaessa aina kohdearkkitehtuuritasolle asti. Tässä nopeasti muuttuvassa ja kehittyvässä kokonaisuudessa kyberturvallisuusuhkien arviointeja ja analyysejä on vaikeaa tehdä

Digitalisointi muuttaa jatkuvasti toimintaympäristöämme nopeasti ja ennennäkemättömällä tavalla. Käyttämiemme laitteiden lukumäärä sekä tiedon määrä tietokeskuksissa ja käytössämme olevissa laitteissa kasvaa eksponentiaalisesti. Tästä syystä sekä energiankulutuksemme että tieto- ja turvallisuusuhat kasvavat myös eksponentiaalisesti.

Lukemattomat internet- ja anturilaitteet, ihmisen hyvinvointia seuraavat laitteet ja tietokoneet voidaan kytkeä käyttäjän matkaviestimeen langattoman tekniikan avulla milloin tahansa. Nämä laitteet toimivat ympäristöissä, joissa käytetään paljon muitakin langattomia laitteita, kuten kodin automaatiojärjestelmiä, kodinkoneita ja kodin turvalaitteita. Näiden laitteiden suojaus ei kuitenkaan ole välttämättä aina riittävä tai sitä ei ole lainkaan.

Energiatehokkuus ja ilmastomuutos ovat kriittisimmät kysymykset ympäristössämme, ja siksi ne on huomioitava käyttämissämme järjestelmissä. Tässä väitöskirjassa esitetään virtualisoinnin, järjestelmien profiloinnin ja nollaenergiaviestinnän avulla tapahtuvaa energiankulutuksen ja hiilidioksidin sekä kasvihuonekaasujen määrän vähentämistä.

Yhdistäessä maanosat merenalaisilla optisilla kaapelijärjestelmillä toisiinsa, kulkee noin 97% mannertenvälisestä viestinnästä niiden läpi. Tämä lisää valtion tasoisten toimijoiden kiinnostusta merikaapelijärjestelmiä kohtaan. Näillä toimijoilla on mahdollisuus kytkeytyä (muodostaa liityntäpiste) myös optisiin merikaapelijärjestelmiin ja kerätä sekä hyödyntää niiden kautta kulkevia tietoja. Meneillään oleva kehitys tarjoaa siten valtavan määrän mahdollisuuksia valtion tasoisille toimijoille, kyberhyökkääjille ja hakkereille hyökätä tätä kautta järjestelmiämme vastaan ja kerätä niissä olevaa tietoa. Ne voivat myös käyttää satelliittijärjestelmiä väärennettyjen tietojen lähettämiseen ja samanaikaisesti käyttää läsnäolonsa piilottamiseen muun muassa TOR-verkkoa. He voivat hyökätä merivalokaapelijärjestelmien kautta toisilla mantereilla oleviin organisaatioihin ja piilottaa jälkensä erilaisilla viestintäratkaisuilla ja väärillä tiedoilla.

REFERENCES

3GPP-5G, https://www.3gpp.org/release-15.

5G Norma, https://5g-ppp.eu/5g-norma/.

5G- PPP, 'Use cases and performance evaluation models', https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-use-cases-and-performance-evaluation-modeling_v1.0.pdf, 2016-04-25.

5G- PPP, '5G-PPP White paper on 5G and e-Health', https://5g-ppp.eu/wp-content/uploads/2016/02/5G-PPP-White-Paper-on-eHealth-Vertical-Sector.pdf, September 2015.

5G- PPP, '5G-PPP White paper on 5G and Energy', https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White_Paper-on-Energy-Vertical-Sector.pdf, Version 1.0 -Date: 30 September 2015.

5G-PPP,'White paper, View on 5G Architecture', *European Commission*, Version 1.0, July 2016.

ABC News, Fears of hackers targeting US hospitals, medical devices for cyber-attacks, Jun 29, 2017.

ARCTIC CIRCLE, https://en.wikipedia.org/wiki/Arctic_Circle.

Arctic Ocean Map and Bathymetric Chart Map, taken from Geology.com, https://geology.com/world/arctic-ocean-map.shtml.

Aurore LE BRIS, Walid EL ASRI, 'State of cybersecurity & cyber threats in healthcare organizations', *Essec Business school*, 2016,https://blogs.harvard.edu/cybersecurity/2017/01/10/cybersecurity-cyber-threats-in-healthcare-organizations/#comment-100.

Azade Fotouh, Ming Ding, Mahbub Hassan,' Service on Demand: Drone Base Stations Cruising in the Cellular Network', *University of New South Wales (UNSW) and Sydney,* Australia, 26 Oct 2017.

Beecham, 'Beecham Research's Sector Map', http://www.beechamresearch.com/download.aspx?id=18.

Beecham Research's, ' Wearable Technology Application Chart´, http://www.beechamresearch.com/download.aspx?id=36.

Beecham Research's, 'World of Connected Devices', http://www.beechamresearch.com/download.aspx?id=18.

Behrang H., Hamadani, Dougherty Brian., 'Solar cell characterization', 2014.

Birkeland Roger., ´An Overview of Existing and Future Satellite Systems for Arctic Communication´, The 4S Symposium 2014.

Brandon Russell, 'UK hospitals hit with massive ransomware attack´, May 12, 2017.

Cheer Chen, ´Fiber Optic Cabling Solutions´, October 13, 2015. http://www.cables-solutions.com/tag/edfa

Chesney Jose, ´Undersea Fiber Communication Systems´, Elsevier ltd, 2016.

Covernment of Canada, Natural Resources Canada, https://www.nrcan.gc.ca/energy/energy-sources-distribution/renewables/about-renewable-energy/7295.

Damiano A., Marongiu I., Musio C., Musio M.,' Concentrator Photovoltaic Standards: Experimental Analyses of Technical Requirements', *Department of Electric and Electronic Engineering University of Cagliari Cagliari*, Italy, IEEE 2013.

Davenport Tara, Submarine Cables, 'Cybersecurity and International Law: An Intersectional Analysis', 24Cath. U. J. L. & Tech (2015). Available at: http://scholarship.law.edu/jlt/vol24/iss1/4.

Dongfeng Fang., University of Nebraska, Lincoln Yi Qian University of Nebraska, Lincoln Rose Qingyang Hu Utah State University,' Security for 5G Mobile Wireless Networks', 12-2017.

Dragon1-open EA Method / Visualization Standard, '*Enterprise Architecture Framework*', http://wigi.dragon1.org.

Electro Power Systems (Aka ENGIE EPS),' Clean Tech Market Leader With 3x Potential Upside Over The Next 24 Months', February, 1, 2019, https://seekingalpha.com/article/4237111-electro-power-systems-aka-engie-eps-clean-tech-market-leader-3x-potential-upside-next-24/.

Ellinger,F., Mikolajick, T,. Wettwies, G., Energy Efficiency enhancements for semiconductors, communications, sensors and software achieved in Cool silicon cluster project', *The European Physical Journal, vol 63, no 1, pp 1 c12*, 2013.

EMP-suojausohje (LM 7/ETS/89, 21.6.1989), https://www.vahtiohje.fi/web/guest/622.

ENISA, 'Security aspects of virtualization', 2017, www.enisa.europa.eu.

ENISA, 'Threat Taxonomy, A tool for structuring threat information', INITIAL VERSION, 1.0, JANUARY 2016.

EPA, The Environmental Protection Agency, '*Report to Congress on Server and Data Center Energy Efficiency*', August 2, 2007, https://www.energystar.gov/ia/partners/prod_development/downloads/EPA_Datacenter_Report_Congress_Final1.pdf.E

EPA, The Environmental Protection Agency, 'Greenhouse Gas Equivalencies Calculator', https://ec.europa.eu/energy/en/publications.

EU- Energy Efficiency Directive, 2012/27.

EU FP7 ICT-317669-METIS, 'Deliverable D1.1 Scenarios, requirements and KPIs for 5G mobile and wireless system, ICT-317669', http://www.metis2020.com/.

EU-GDPR, The General Data Protection Regulation, 2016/679.

EU- MDR, The Medical Devices Regulation, 5/2017.

EU- NIS, ´Concerning measures for a high common level of security of network and information systems across the Union´, 6/2016.

European Parliament and of The Council, 'The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing', Directive 2016/679, 27.5.2016.

European Parliament and of The Council, 'Energy efficiency', 25.10.2012.

Finland´s Cyber Security Strategy (2013) Government Resolution, Finland.

Fitch, S.C. A. Muckin, M, 'Threat-Driven Approach to Cyber Security, Methodologies, Practices and Tools to Enable a Functionally´, Integrated Cyber Security Organization', 2015, Lockheed Martin Corporation.

Flink Jari-Pekka, Diplomityö, ´Uusiutuvan energian hyödyntämismahdollisuudet Nurmi-Sorilan alueen suunnittelussa (Tampere)´.

Foster Ian Armas., ´NIST's Security Reference Architecture for the Cloud-First Initiative´, June 28, 2013.

Geology.com,' Arctic Ocean Seafloor Features map', https://geology.com/articles/arctic-ocean-features/.

Hansen/UMD/Google/USGS/NASA, Global Forest Wacth, Tree Cover Loss, http://data.globalforestwatch.org/datasets/63f9425c45404c36a23495ed7bef1314.

Hanna Hoag, ´Getting Renewable Energy into Remote Communities´, *Newsdeeply*, April 26, 2016, https://www.newsdeeply.com/arctic/community/2016/04/26/getting-renewable-energy-into-remote-communities.

Heinzmann, P. Steffen, A. 'The Hacking Cycle´, *Institute for Internet Technologies and Applications*, 2012, Italy.

Helferich. A, Herzwurm. G, Schocker. S, ´The use of Quality-Function Deployment (QFD)for customer-focused Product Development´.

Hobart M. King, Ph.D., RPG, Arctic Ocean Seafloor Features Map, Major Basins, Ridges, Shelves and Bathymetry, Geology.com, 2016.

Hobart M. King, Ph.D., RPG, Oil and Natural Gas Resources of the Arctic, https://geology.com/articles/arctic-oil-and-gas/.

Holdmann Gwen, Written Testimony before the United States Senate Committee on Energy and Natural Resources, Alaska Center for Energy and Power University of Alaska Fairbanks, June 10th, 2017, https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=C826A2CE-FC8C-4C92-BA49-ECE5451872DD.

Hummelholm, Aarne., 'DWDM-TEKNIIKKAA TIEDONSIIRTOVERKOISSA', 12.6.2000, Teknillinen korkeakoulu, Sähkö- ja tietoliikennetekniikan osasto.

Hummelholm, Aarne., 'WDM-TEKNIIKKA N-ISDN-TILAAJAVERKOISSA', TEKNILLINEN KORKEAKOULU, Sähkö- ja tietoliikennetekniikan osasto, S-72.173 (3 ov) (1997 -1998).

Hummelholm Aarne, 'S-72.4210 Postgraduate Seminar on Wideband Radio, Communications Laboratory', 31.1.2006.

Huttunen, H. L., Halonen, R., Koskimäki, H. ´Exploring use of wearable sensors to identify early symptoms of migraine attack´, 2017, September.

Huttunen, H. L., Halonen, R. ´Preferred Biosignals to Predict Migraine Attack 2018, September).

Huttunen, H. L., Halonen, R. (2018), ´Willingness to Use Smartphone Application Assistant to Support ITU-T, Security in Telecommunications and Information Technology´, September 2015.

Hämäläinen, Juhani., Järviö Petri., Kuja-Halkola Sami., Silvola Perttu., Paunonen Jari.,' Sähkömagneettisten aseiden teknologiaa', *Defence Forces Technical Research Centre*, RIIHIMÄKI 2009, ISBN 978-951-25-1991-0 (nid), ISBN 978-951-25-1994-1 (PDF), ISSN 1457-3938.

IEC 61646, Thin-Film PV Modules.

IEC, 'Orchestrating infrastructure for sustainable Smart Cities', *White paper*, Geneva, Switzerland 2014, info@iec.ch, www.iec.ch.

IEEE -11073-10419, Insulin Pump.

IEEE – 11073-10417, Glucose Meter.

IEEE -802.11, WiFI.

Insights Success, 'Green Cloud Computing: Saving Energy through Technology', 2019, https://www.insightssuccess.com/green-cloud-computing-saving-energy-through-technology/

Istepanian Robert S. H., Woodward Bryan., ´m-Health, Fundamentals and Applications´, Wiley, 2017, ISBN: 978-1-118-49698-5.2017.

ITU-T, G.709/Y.1331, Interfaces for the optical transport network, 6/2016.

ITU-T, G.971, General features of optical fibre submarine cable systems, 11/2016.

ITU-T G.977 (01/2015).

ITU-T, Manual 2009, Optical fibres, cables and systems.

ITU-T, Spectral grids for WDM applications: DWDM frequency grid, G.977 (01/2015).

JHS 179, 'Enterprise architecture planning', Modified date 2018-01-30, http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/179.

Joensuu, Jukka-Pekka., ´Navigating the Arctic´, 13 th February 2018, http://asia.blog.terrapinn.com/submarine-networks/2018/02/13/navigating-the-arctic/.

Kaushik Pal, 'How Green Computing Can Improve Energy Efficiency in IT ',March 2017, https://www.techopedia.com/how-green-computing-can-improve-energy-efficiency-in-it/2/32212.

Kent Jaimie, ´Geopolitical Implications of the Melting Arctic Ice Cap´, Are States Doomed to Conflict or Convinced to Cooperate? Illinois State University, 2015.

Khajuria Samant., Sorensen Lene., Skouby Knud Erik., ´Cybersecurity and Privacy Bridging Gap´, River Publishers, 2017.

Khan A.S., Javed Yasir., Abdullah J., Nazim J.M., Khan N., 'Security issues in 5G device to device communication', *IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.5*, May 2017.

Limnell, J. Majewski, K. Salminen, M. 'Kyberturvallisuus', Docento Oy, 2014, Finland.

Max Power, Global Geomagnetic Storm Induced Failure of 400 Mega-HVAC Transformers is Avoidable by Redundant HVAC Transformer Arrays, http://hireme.geek.nz/solar-storm-hvac-transformer-avoidable-failure.html, 24,October, 2009, last modified 24 may 2014.

M-Files,' Intelligent Information Management Platform', https://www.m-files.com/en.
METIS 2020, https://5g-ppp.eu/white-papers/.

Mitre, 'The common weakness enumeration, A Community- Developed Dictionary of Software Weakness Types, CWE version 3.0', 2017, http://cwe.mitre.org/data/published/cwe_v3.0.pdf.

MITRE, 'GETTING STARTED WITH ATT&CK', 2019, https://www.mitre.org/publications/technical-papers/getting-started-with-attack.

Miyamoto Yutaka, Kawamura Ryutaro, NTT Technical Review, Feature Articles: State-of-the-art Space Division Multiplexing Technologies for Future High-capacity Optical Transport Networks, ΄Space Division Multiplexing Optical Transmission Technology to Support the Evolution of High-capacity Optical Transport Networks΄, Vol. 15 No. 6 June 2017.

OLEG V ,'Green Computing – Technology of the Future', MAY 28, 2011, https://us.ecocompass.com/blog/green-computing-technology-of-the-future.

Osborne Hilary., Devlin Hannah., Barr Caelainn.,'Thousands of patients around the world have been damaged by incorrect medical devices', *The Guardian*, 25.11.2018, https://www.nbcnews.com/health/health-care/how-can-medical-device-deemed-unsafe-another-country-still-be-n938706.

Pazowski, Piotr., 'GREEN COMPUTING: LATEST PRACTICES AND TECHNOLOGIES FOR ICT SUSTAINABILITY', *Maria Curie Skłodowska University,* Poland, 2015, http://www.toknowpress.net/ISBN/978-961-6914-13-0/papers/ML15-377.pdf.

Population centres in the north, https://www.arcticcentre.org/EN/communications/arcticregion/Maps/Cities.

Public Private Partnership (5G PPP), 'The 5G Infrastructure the next generation of communication networks and services', www.5g-ppp.eu.

Puolustusministeriö, ´Katakri-2015, Tietoturvallisuuden auditointityökalu viranomaisille´, https://www.defmin.fi/julkaisut_ja_asiakirjat.

QFD INSTITUDE, 'The official source for QFD, Quality Function Deployment (QFD)', http://www.qfdi.org/what_is_qfd/what_is_qfd.htm.

Ramjee Prasad., 5G Outlook, Innovations and Applications, River Publishers, 2016.

Reddit, Map Of Underwater Cables That Supply The Worlds Internet, 30 September 2017, www.reddit.com/r/MapPorn/comments/73ekox/map_of_underwater_cables_that_supply_the_worlds/.

Renewable Energy Institute,' Renewable Energy Technologies', http://www.congenetation.net/.

Robert, 'Underwater volcanoes melting Arctic Ice, says geologist´, January 20, 2016January 20, 2016 https://www.iceagenow.info/underwater-volcanoes-melting-arctic-ice-says-geologist/.

Schmarzo, Bill.,'Autonomous to Smart: Importance of Artificial Intelligence', AI/IOT/ANALYTICS, Dell Technologies, July 19, 2017, https://infocus.dellemc.com/william_schmarzo/autonomous-smart-artificial-intelligence/.

Shiel Fercus., 'About The Implant Files Investigation', November 25, 2018, https://www.icij.org/investigations/implant-files/about-the-implant-files-investigation/.

Shishir Kumar Shandilya, Soon Ae Chun, Smita Shandilya, Edgar Weippl, 'Internet of Things Security, Fundamentals, Techniques and Applications', River Publisher, 2018, ISBN: 978-87-93609-53-2.

Small Nuclear Power Reactors, http://www.world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/small-nuclear-power-reactors.aspx.

martCitiesCouncil,' SMART CITIES READINESS GUIDE, The planning manual for building tomorrow's cities today', 2013 SMART CITIES COUNCIL, James.Whittaker@SmartCitiesCouncil.com.

STAT, *By* ASSOCIATED PRESS, 'Medical devices for pain, other conditions have caused more than 80,000 deaths since 2008', November,25,2018,https://www.statnews.com/2018/11/25/medical-devices-pain-other-conditions-more-than-80000-deaths-sice-2018/.

Syed Fahad Yunas, 'Capacity, Energy-Efficiency and Cost-Efficiency Aspects of Future Mobile Network Deployment Solutions', *Tampere University of Technology, 9th of October* 2015, ISBN 978-952-15-3581-9 (printed, ISSN 1459-2045.

Takahashi, Dean., 'Drones and fiber-optic attacks may threaten security for Super Bowl 50', January 18, 2016. https://venturebeat.com/2016/01/18/super-bowl-50-security-wont-be-easy-to-pull-off-in-the-age-of-drones-and-fiber-optic-attacks/.

Teec David J., '5G Mobile: Impact on the Health Care Sector', October 26th, 2017.

THE ARCTIC, https://arctic.ru/population/.

The University of Alaska Fairbanks, The Alaska Center for Energy and Power (ACEP), Developing practical, cost-effective energy solutions for Alaska and beyond, http://acep.uaf.edu/.

Threats to Undersea Cable Communications, PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM, September 28, 2017.

Traficom, Viestintävirasto, Kyberturvallisuuskeskus, 'Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista', 20.12.2018. 26. EMP-suojausohje (LM 7/ETS/89, 21.6.1989), https://www.vahtiohje.fi/web/guest/622.

University of Cambridge, 'Cost - Benefit - Risk Analysis', https://www.ifm.eng.cam.ac.uk/research/dstools/cost-benefit-risk-analysis/.

Vanhanen Mika, 'ENO PROGRAMME ASSOSIATION', https://sites.google.com/a/enoprogramme.org/eno-verkkokoulun-tuki-ry/Home.

Viestintävirasto, 'Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista´, Helsingissä 17 päivänä joulukuuta 2014, (917/2014) 244 §.

Wang, P., Liu, J.C., 'Threat Analysis of Cyber- attacks with Attack Tree +', 2014.

Ye Yincan, Jiang Xinmin, Pan Guofu, Jiang Wei,' Submarine Optical Cable Engineering', Elcevier Inc. 2018.

Yutaka Miyamoto, Ryutaro Kawawura, ´Space Division Multiplexing Optical Transmission Technology to support the Evolution of High-capacity Optical Transport Network´, June 2017.

APPENDIX 1.

The energy efficiency of Data Centers

Aarne Hummelholm, Technical Manager
Ministry of Finance
Helsinki, Finland
aarne.hummelholm@elisanet.fi,

ABSTRACT

The purpose of this presentation is to describe the situation concerning energy consumption of data centers and communications networks according to the current situation, as well as to present alternative solutions to more efficient future data centers environments and communications network systems when it comes to energy consumption.

The presentation provides several possibilities for reducing energy consumption with different solutions involved in and influencing the physical infrastructure of data centers as well as solutions concerning the actual architectural issues and technical issues of the hardware.

The goal is to create an image of future data center solutions, which enable optimization of energy consumption and yet an effective operation of data center environments for producing services in secured operations environments. This presentation is focusing more ideas than exact calculations of savings. Accurate savings are very difficult to calculate, because equipments new investments values after five to ten years is very difficult to guess right.

INTRODUCTION

The range of the teleservices people need every day grows constantly, and the operational environments needed by the service providers grow along with it, if not even faster. In today's world, people want teleservices where ever they go, even as a real-time service, no matter the costs.

People want to connect to the Internet whenever they want, read their e-mails anywhere, listen to music whenever they feel like it, and watch movies from their computer, regardless of time and place. New social services have made people even more dependent on computers, information technology and the services it provides. They play different kinds of computer games via the Internet or spend time in Facebook telling about their day to others. It is possible to live in a virtual world, when you have time and desire to escape from reality. People have become addicted to information technology. IT (Information Technology) changes people's operational environments, people themselves, and service supply.

In addition, it provides opportunities to operate in a new way and frees time for oneself and one's hobbies.

In the commercial world, electronic commerce, banking and stock market also grows faster than ever.

In the corporate world, people want to simulate different kinds of things, verify the functionality of systems before implementation, model things with 3D (Three Dimensions) models and produce different products with moving pictures for commercials, for instance for the Internet starting page. There are an infinite number of different kinds of service forms, which need more network and server resources in order to work. In addition, service producers constantly try to come up with new appealing services, so that they would gain better results and, thus, develop their own operations.

All of the above means additional requirements in the data centers spaces of service producers as increased data processing capacity, growing number of servers, capacity requirements of information saving systems and an increased need of telecommunications capacity as well as an increased need of space.

THE CHALLENGES OF DATA CENTERS AND TELECOMMUNICATIONS

Different services of information technology and the powerful growth in resulting telecommunications have surprised the telecommunications companies, service producers as well as operators in charge of service environments and data centers.

When offering different kinds of new teleservices to people, no one has considered the aggregate widely enough, and, thus, we have drifted to the current situation – nothing is enough.
The growth in the amount of offered services increases the data centers' hardware base, telecommunications equipments, servers, storage systems, and data security equipments. This, in turn, increases thermal stress.

The thermal stresses of data centers are out of control. Their inner spaces are inadequate, recording capacity is insufficient, and delivering the services is not, in all circumstances, flexible and trouble-free. At the same time, the need for energy in data centers increases to such massive amounts that no resources seem to be enough, Image 1.

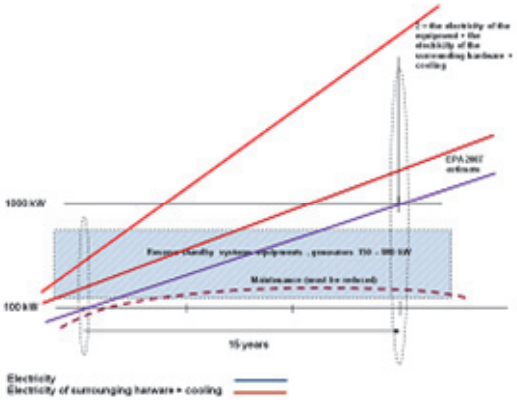


Image 1. The increase prognosis of the energy need of data centers in case no change is made compared to the current situation [1] [2].

As the evaluation of the United States' will EPA (Environmental Protection Agency) shows, the energy requirements of data centers increase about ten-fold during the next 15 years [2]. This is due not just because of fulfilling the energy need of the equipments inside the data centers, but cooling the routers takes up even more electrical energy than the routers themselves. The router manufacturer Cisco predicts an even larger growth. According to their estimate, the energy need of data centers will grow to about 17-fold in the next 15 years [1].

As a result, large data centers need to be built in areas where there is enough energy available even 15 years on from now. One possibility is building an own power plant next to the data centers.
Although the energy efficiency of appliances and the components used in them increases, the growth of energy requirements still remains large. In Image 1, this increase in the energy efficiency of components has already been taken into account.

THE DEVELOPMENT OF DATA CENTERS

All over the society, the huge rise in energy consumption (Image 1) has brought forth new ideas for reducing energy consumption and making it more efficient. This is called 'Green IT'.

Green IT contains the reduction of energy consumption and energy saving, observation of the carbon footprint in all operations, and reduction of the amount of emissions. It contains new operational models, which are meant to influence people's behavior and consumer habits in order to reduce greenhouse emissions and save energy.

These values are the central concepts of Green IT when planning new data centers spaces and restoring the old ones to fulfill new requirements.

The equipment systems of the current data centers have still, in part, been built from individual network components, individual servers and server groups as well as storage systems. Each system still has its own control and monitoring equipment with its own monitoring personnel.

In addition, the energy consumption is not measured accurately enough, so the realization of energy savings is not properly brought out.

VIRTUALIZATION

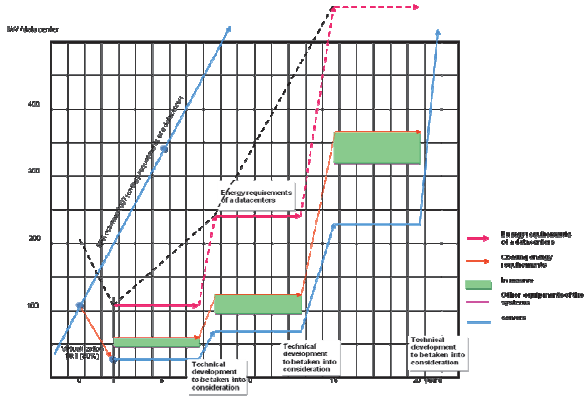


Image 2. An example of the advantages in energy saving attained by virtualization of data centers.

In order to reduce energy costs and secure the operations of data systems, virtualization has become a new central technique when we search for efficiency for the operations of data centers, reducing possibilities of the number of equipments, reduced energy consumption and cost savings.

Almost all functions inside data center can be virtualized, except for the physical equipment environments required by the virtual machines [3] [4] [5] [6] [7].

Servers, storage systems and telecommunications can be virtualized. The servers can even be virtualized on a ratio of

10/1 by using 80% utilization rate, in case of which we do not yet weaken the performance needed by the service.

If, for instance, the servers are virtualized 10/1, savings will be made in equipment costs; license, update and maintenance costs; cabling and connector costs as well as energy costs (Image 2). The cost savings can be directly calculated from the degree and amount of virtualization. In addition, the need for space reduces. We can also make virtual backups of systems and servers. In this case, we make a virtual copy of the system and run it in another virtual environment of data centers environment [8] [9].

An example of virtualizations:

As an example, let us assume that we have 1,000 servers in use, and these can be virtualized 10/1 by using 80% utilization rate. In the calculations, we have used modified prices which correspond in amount to actual prices.

Servers:
The price of a non-virtualized server = €4,000
The price of a virtualized server = €5,000
The total price of a non-virtualized server environment = €4,000,000
The price of a virtualized server environment = €500,000

Energy consumption, non-virtualized environment:

A non-virtualized server uses energy 345.5W
The total energy consumption of non-virtualized servers: 345,500W
Total consumption / year ∑ = 345,500W x 24h x 365 days = 3,026,580kWh/year
Total cost / year ∑ = 3,026.58MWh/year x €100/MWh = €302,658/year

Cooling and other surrounding hardware in a data center take up, in practice, two times the energy amount required by the appliances (year 2006) or 2 x 3,026,580kWh/year or 6,053,160kWh/year. Total costs of cooling and surrounding hardware / year ∑ = 6,053.160MWh/year x €100/MWh = €605,316/year. Energy costs in this example calculation in a non-virtualized environment = €907,974/year.

In addition, maintenance, software updates and license fees need to be paid for the servers annually. Usually, they are about 18% of the acquisition price, depending on the sales contract. On this basis, an annual cost for a non-virtualized environment is the following total amount:

Annual maintenance costs ∑ = 18% x €4,000,000/100 = €720,000/year

Energy consumption, virtualized environment:

A virtualized server consumes energy 384W
Total energy consumption of virtualized servers = 38,400W
Total consumption / year ∑ = 38,400W x 24h x 365 days = 336,384kWh/year
Total costs / year ∑ = 336.384MWh/year x €100/MWh = €33,638/year

Cooling and other surrounding hardware in a data centers take up, in practice, two times the energy needed by the routers (year 2006) or 2 x 336,384kWh/year or 672,768kWh/year ([2]).
Total cost / year of cooling and surrounding hardware ∑ = 672,768MWh/year x €100/MWh = €67,276.8/year.
Energy cost in this example calculation in a virtualized environment = €100,914.8/year

Examples of the advantages in energy savings and costs savings by virtualization of servers in data center.

Virtualizations environments	Non-virtualized servers, 1000 servers	Virtualized servers, 100 servers	Savings in virtualization
Price of Server, €	4000	5000	
Total price of Servers , €	4.000.000	500.000	3.500.000
Energy consumption / server (W)	345.5	384	
Total consumption, kWh/ year	3.026.589	336.385	2.690.204
Total energy costs, €/ year	302.658	33.638	269.020
Cooling + other surrounding hardware, energy consumption, kWh/ year	6.053.160	672.768	5.380.392
Cooling + other surrounding hardware, energy costs, €/ year	605.316	67.276	538.040
Total costs of energy, €/year	907.974	100.914	807.060
Maintenance costs, €/ year	720.000	90.000	630.000
Total energy consumption, kWh/ 5 years	15.132.945	1.681.925	13.451.020
Total energy costs, €/ 5 years	4.539.870	504.570	4.035.300
Savings in maintenance costs, €/ 5 years	3.600.000	450.000	3.150.000
Savings in equipment costs, €/ 5 years			3.500.000
Savings in energy costs, €/ 5 years			4.035.296
Savings in maintenance costs, €/ 5 years			3.150.000
Savings in total, €/ 5 years			10.685.296

Table 1. Examples of the advantages in energy savings and in costs savings by virtualization of servers in data center, summary table.

Annual maintenance costs in accordance with the previously presented model are as follows:

Annual maintenance costs ∑ = 18% x €500,000/100 = €90,000/year

Savings achieved by virtualization in this example are as follows:
- equipment costs, savings are €3,500,000
- energy costs (other equipments, cooling, and surrounding hardware) savings are €807,059.2/year
- maintenance costs (licenses, updates and maintenance) savings are €630,000/year

We can also consider the subject for a period of five years, since servers need to be changed approximately every five years. In this case, savings are as follows:

- savings in equipment costs = €3,500,00 / 5 years
- savings in energy costs = €4,035,296 / 5 years
- savings in maintenance costs = €3,150,000 / 5 years

Virtualization 10/1, utilization rate 80%, in environments of 1,000 servers upwards the total savings from equipment, energy and maintenance are €10,685,296 / 5 years.

Examples of the advantages of CO_2 (Carbon Dioxide, Greenhouse gas) savings conserning servers virtualization.

Greenhouse gas savings	Energy savings kWh/year	CO_2 savings, Tons
Savings / year	2.690.204	2.130
Savings / 5 year	13.451.020	10.648

Table 2. Greenhouse gas savings in virtualizations, summary table.

PROFILING OF THE DATA CENTERS

Since the need and use of services differs during different times of the day, and not all services are needed during the night, the data centers can be profiled on the grounds of the utilization rate and the required critical applications. This is a whole new way of reducing the energy consumption of data centers.

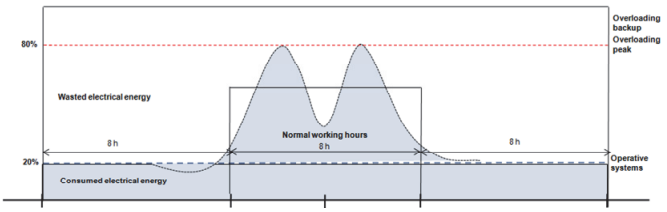


Image 3. The distribution of services during the day.

This solution can save considerable amounts of energy. For instance, let us assume that the utilization rate of a data center of 1MW would be reduced during the night near standby with regards to certain services, whereas critical functions stay on (Image 3). The system can be on standby even for over ten hours without weakening the level of service. If, for instance, the power of a data center can be cut down by 800kW, even this will bring energy savings of 12,800kWh for one day. In addition, the data center can be profiled so that also the load variations during a day can be taking care. In this way, the potential savings are considerably higher.

Energy savings in a day ∑ = 800kW x 16h = 12,800kWh/day

Savings can also be considered on a weekly basis. People do not usually work on Saturdays and Sundays, so the data center can be on standby for the whole weekend. In this case, the total energy savings for the weekend are 38,400kWh on a load of 200kW. Total savings for the whole week are 102,400kWh. On an annual level, this means savings of 5,324,800kWh in electrical energy. Financial savings are (according to €100/MWh) €532,480/year.
Energy savings in a week ∑ = (800kW x 16h) x 5 days + (800kW x 48h) = 102,400kWh/week
Energy savings in a year ∑ = 102,400kWh/week x 52 weeks= 5,324,800kWh/year
Financial savings in a year ∑ = 5,324,800kWh/year x €100/MWh = €532,480/year
Financial savings in five years ∑ = €532,480/year x 5 = €2,662,400 / 5 years

In order for the profiling of data centers to work properly, an integrated data center control and monitoring system is required. With the help of a control system, in the future the services can be directed to standby even on an accuracy of individual services. The system has to be scalable, as well. With this kind of a solution, we can also cut down individual control and monitoring instances, make the operations more effective as well as save energy.

When the data centers have been profiled, energy savings can also be gained by profiling the users' hardware. For instance, if an organization has 10,000 employees with their own work stations, and the electrical energy consumption is on average c.100W / work station, the total electrical energy consumption of the corporation is 1,000kW on the basis of the work stations alone. This means 7-8MWh / work day / 10,000 employees, if the work stations are turned off or are in a power saving mode during the night. If they are locked, as they often are during the night, energy is wasted. There are programs, with which work stations on standby can be turned on, for example, for the duration of updates, after which they return to standby. At worst, the energy consumption would be 24MWh/day, if the work stations are constantly on with the presented work station load.

The energy consumption of work stations without power saving mode ∑ = 24MWh/day x 365 = 8,760MWh/year
The energy invoice of work stations in a year ∑ = 8,760MWh/year x €100/MWh = €876,000/year
If the work stations are turned off during the night, the energy invoice in a year (Image 3) is the following sum.

On standby, the work station consumes less than 10W. For the work stations of 10,000 employees, this means a

consumption of 100,000W during the night. The total savings during the day will be ∑ = 90W x 10,000 x 16h = 14.4MWh/day
Energy savings in a week ∑ = 14.4MWh/day x 5 days + (90W x 10,000 x 48 h) = 115.2MWh/week
Energy savings in a year ∑ = 115.2MWh/week x 52 weeks = 5,990.4MWh/year
Financial savings in a year ∑ = 5,990.4MWh/year x €100/MWh = €599,040/year
Financial savings in five years ∑ = €599,040/year x 5 = €2,995,200 / 5 years.

Examples of the advantages in energy savings and costs savings by profiling of data centers and work stations.

Energy use and savings by profiling Date Centers and work stations	Data centers energy use	energy use of 10.000 employees workstations
Working time (h)	8	8
Leisure time (h)	16	16
Electricity use, kW (max)	1000	1000
Electricity savings, kW	800	900
Energy use, kWh/ day	24.000	24.000
Energy savings, kWh/ day	12.800	14.400
Energy savings, kWh/week	102.400	115.200
Energy savings, kWh/years	5.324.800	5.990.000
Financial savings, €/ week	10.240	11.520
Financial savings, €/ year	532.480	599.040
Financial savings, €/ 5 years	2.662.400	2.995.200

Table 3. Examples of the advantages in energy savings and costs savings by profiling of data centers and work stations, 8h (100% load) and 16h (20% load in data center), summary table.

Examples of the advantages of CO_2 savings by profiling Data Centers and work stations.

Greenhouse gas savings	Energy savings kWh/ 5year	CO_2 savings, Tons
Data centers savings	5.324.800	4.215
Work Stations savings	5.990.000	4.742

Table 4. Greenhouse gas savings by profiling Data Centers and work stations, summary table.

When the savings also include printers and copy machines, the energy saving entity of the organization will be in control and information technology can be developed as a whole by taking Green IT and energy saving possibilities into account.

TRANSFORMING WASTE ENERGY INTO COOLING ENERGY AND ELECTRICITY

A completely new idea in reducing the energy consumption of data centers is the possibility of utilizing the waste heat of data centers in cooling them. The innovation is based purely on classic physics. Image 4 shows the influence of this in the total energy consumption of data centers.

Data centers produce large amounts of thermal energy which goes to waste. Utilizing and recycling this wasted energy would reduce the energy need, use costs and also the renewal need of the surrounding hardware of data centers.

Preliminary research shows that more than 70% of the waste heat could be utilized by changing it back to cooling energy. Even this result is better than not utilizing the waste heat at all. The aim is to reduce the need of intake energy of data centers, and, thus, lower the costs as well as the need for electrical energy.
This is also of great significance internationally, if the waste heat of each data centers can be utilized by even over 70% efficiency and, in addition, the energy need of data centers cut down during the night. Previously, households could use by night time electricity, which was cheaper than daytime electricity. This solution also leveled the electricity consumption during the day. We should only find the right ratio between the use of night time and daytime electricity [10] [11].

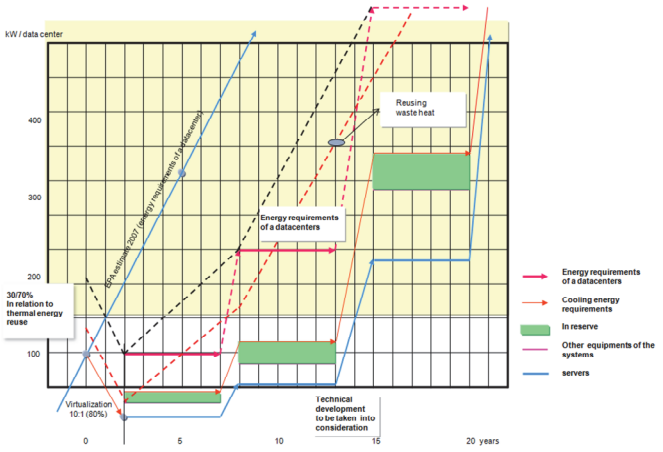


Image 4. An example of energy savings attained by reusing the wasted thermal energy of data centers with CCHP systems (combined cooling, heating and powering) .

If we assume that a country has, for example, 20 data centers of 1MW, then they need 20MW for the energy of the hardware alone. If we then calculate the amount of energy required by the data centers and the surrounding hardware, the energy need is approximately 40MW [2], of which the portion of the cooling energy is about 20MW.

If we can utilize 70% of the waste heat produced by a data center, we can utilize 14MW of the cooling energy of 20MW again as cooling energy. At the same time, we can reduce the amount of input power of the data centers and gain savings in costs.
As an example, we can calculate what this means in terms of expenses.

20MW of energy means during the day 480MWh/day.
On an annual level, the energy consumption is 175,200MWh/year.
If we can reuse 70% of this amount of energy, it means 122,640MWh.
The cost of the reusable energy is €12,640,000/year.
Financial cost in five years ∑ = €12,640,000/year x 5 = €63,200,000 / 5 years

In the calculations, it has been assumed that building the data centers is done with the principles according to Image 2.

The obtained result can be examined in accordance with Image 1 for the whole period of 15 years. In the image, the energy consumption increases 10-fold during a period of 15 years. When we do not take index increases into account, the financial cost of the previously calculated sum for 15 years will be €189,600,000 / 15 years, calculated merely on the basis of the starting situation.

But energy consumption has increased after five years and, during that time, has already doubled, so the need for cooling energy has also doubled. The same applies for the next period of five years, when the consumption is three times the starting value.

Calculated on this basis, the financial cost of the reusable energy during the next period of five years is ∑ = €63,200,000 / 5 years x 2 =€126,400,000 / 5 years.

Respectively, the cost of reusable energy for the next period of five years is ∑ = €126,400,000 / 5 years x 3 = €379,200,000 / 5 years.

The financial cost of the reusable energy for the whole period of 15 years is €568,800,000 / 15 years calculated according to the values of images 2 and 4. Even if the virtualization of data centers would be executed in accordance with Image 2, we would still need cooling energy.

Costs in savings are enormous. At the moment, there are already 52 web data centers in Finland [12]. When we add the data centers owned by organizations to this, reusing even this waste heat and with these efficiencies we will gain enormous savings on an annual basis. It is difficult to find out more specific numbers of data centers.
New type of integrated cooling, heating and power systems payback is about 3 to 5 years.

Also a wholly new idea is transforming waste heat directly to electrical energy. This solution and innovation is also based purely on classic physics. This solution has not yet been applied to data centers. The technique has been developed, among others, to satisfy the energy needs of space ships.
This solution can further improve the energy efficiency of data centers, by utilizing the remaining waste heat and transforming it directly to electrical energy.

Transforming waste heat into electrical energy can, at present, be done with the help of Peltier elements, but the efficiency is not very high [13].
Better solutions are sought from the applications of nanotechnology, means of which waste heat can directly be transformed into electrical energy. Nano pipes are one of the most promising transforming elements in this model [14. In addition, nanowire seems to be another efficient energy transformer of the future for transforming heat energy directly into electricity [15].

In the United States, the army is exploring the possibility of utilizing the heat energy of exhaust pipes of heavy trucks in recharging batteries. Technical solutions are available and they can be directly utilized in transforming heat energy into electricity. These solutions have not yet been applied to data centers environments [16].
In both alternatives, the acquisition costs and life cycle costs of the techniques need to be considered in order to calculate the eventual benefit.

Examples of the advantages in energy savings and costs savings by transforming waste energy into cooling energy of data centers, summary

Reusing the wasted thermal energy	Data centers
Electrical energy use for cooling, kW (max)	20.000
Cooling energy use, kWh/day	480.000
Cooling energy use, kWh/ year	175.200.000
The wasted termal energy reusing (70 %), kWh/ year	122.640.000
Thermal energy reusings financial savings, €/ year	12.264.000
Thermal energy reusings financial savings, €/ 5 years	61.320.000
Thermal energy reusings financial savings, €/ 15 years , (Image 4)	183.960.000

Table 7. Example of energy savings attained by reusing the wasted thermal energy of data centers (70 % reuse), summary table.

THE ADVANTAGE FROM REUSING THE WASTED THERMAL ENERGY

If we review the electrical energy used by the United States in 2006 in data centers, which is 61,000,000,000kWh/year [3], the amount of cooling energy is then about 20,000,000 MWh/year. If we can reuse 70% of this, or 14,000,000 MWh/year, we are talking about enormous savings in energy and costs purely on an annual level.

The financial value of the saved energy during a year is an estimated €1,400,000,000/year (€100/MWh)

Examples of the advantages of CO_2 savings by reusing the wasted thermal energy table.

Greenhouse gas savings	Energy savings kWh/year	CO_2 savings, Tons
Data centers used energy	175.200.000	138.695
Reused wasted thermal energy	122.640.000	97.087

Table 8. CO_2 g reenhouse gas savings by reusing the wasted thermal energy, summary table.

THE DEVELOPMENT OF THE ENERGY SUPPLY OF DATA CENTERS, WIRELESS NETWORKS AND COMMUNICATIONS NETWORKS

If we would use direct voltage as the power-supply voltage of data centers, wireless networks and telecommunications networks' hardware, this would erase, among others, the need for UPS in data centers. Using direct voltage also improves the efficiency of energy supply. In the execution, we could leave voltage conversions out of the energy supply system, which means more efficiency. The efficiency can be improved by over 10% [2] [13] [14] [15] [16].

At the moment, the obstacles in the way of technical development are commercial aspects rather than technical solutions.

We can take a 1MW data centers as an example. When we count the effect of a 10% efficiency improvement value to the energy consumption, the resulting value is 100kW. Although at first glance the sum seems small, the energy savings during the day are as much as 2,400kWh/day.

In a year, this results in energy savings of 876,000kWh/year (an example).
Thus, financial savings on an annual level are €87,600 (€100/MWh).

Financial savings in five years ∑ = €87,600/year x 5 = €438,000 / 5 years

This money can be used in acquiring physical server resources, which can be utilized with the help of virtualization, as previously mentioned in section 3.2. This, in turn, considerably increases the advantages gained from improving the energy supply, when reviewing the matter as a whole. The point comes across well in the previously calculated example.The direct voltage system can also be executed as a hybrid solution, in which case solar power, energy cells (previous fuel cell technique), biofuel systems, wind power and other renewable energy forms can be integrated into it. This entity will reduce dependency from imported fuels and, at the same time, the energy supply systems will be considerably more reliable than they currently are.

Examples of the advantages in energy savings and costs savings by the development of the energy supply of data centers.

Table 9. Examples of the advantages in energy savings and costs savings by the development of the energy supply of data centers (DC-systems, direct voltage systems), summary table.

ENERGY EFFICIENCY OF DATA CENTERS

The energy efficiency of data center is a criterion, which is used to define the performance of a data center. The energy efficiency of a data center is defined with DCiE value (DCiE = Data Centre infrastructure Efficiency). The DCiE value is the relation between the power of the IT equipment and the overall power of the data centers [7] [8]. With this value, we can compare the energy efficiency of different data centers very precisely. Therefore, energy measuring systems need to be designed into the data centers, so that the DCiE value can be properly measured. Another term used in measuring energy efficiencies is PUE (PUE = Power Usage Effectiveness). DCiE is 1/PUE.

CONCLUSION

In data centers, communication stations of telecommunications networks and base stations of wireless networks, there are a lot of above-mentioned improvements that can be made in regard to energy saving.

Some of the presented savings models are wholly new solutions, which have not yet been applied, at least on a larger scale, in Finland for data centers, communications stations of telecommunications networks or base stations of wireless networks.

European countries can also save tens or even hundreds of millions of Euros in a year with these solutions.

In addition, and telecommunications networks are not the only places, which form waste heat that is not utilized at all, but these also include, for instance, factories, oil refineries, power plants as well as all structures that produce heat.

Even with all the talk in the world of recycling and reusing materials as well as collecting paper, carton, metal, glass and equipment scraps for reuse, still the recovery of waste heat is minimal.

However, there are enormous savings to be made in reusing waste heat, in Finland and in other countries, as well. The financial savings are tremendous. If we can implement the presented energy saving possibilities, even in part, we can also save immense amounts of funds in building power plants and other energy producing institutions as well as in carbon footprints nationally and worldwide.

The electrical energy of ITC systems and equipment is only a few per cents of the overall consumption of electrical energy in the world. We can only roughly estimate the overall amount of produced waste heat in the world, and this goes directly to the atmosphere to heat the air. The amount of energy in the waste heat can be billions of kilowatt-hours for every use hours worldwide. No matter how clean the waste heat is it still heats the atmosphere. Just like pollution is carried with air currents from one place to another, so does this waste heat, by warming the atmosphere. Where and how this waste heat released into the atmosphere can dissolve, so it would not heat the Earth's atmosphere? According to the law of indestructibility of energy it goes as a whole to some place, where it does not necessarily belong to, and causes its own addition to the warming of the atmosphere.
What are the climatic influences of waste heat directly released into the air? This cannot even be estimated without extensive research.

What we can do for energy savings now and the future are that we start to design whole infrastructure of society taking care of energy saving possibilities, recycling and reusing wasted thermal energy, optimise and profile communications networks, communications stations and data centers.

SOURCES:

[1] Jan Linström, Data Center present and Future Directions, Cisco
[2] Reijo Mäihäniemi, CEO and President of Efore, ICT Getting Green, Efore, 14.10.2008
[3] Keijo Niemistö, Ympäristöystävällinen IT, TTL 3.4.2008, VMware - Energian säästöä palvelinten virtualisoinnilla, VMware Finland
[4] Tomi Jalonen, Cisco Unified Computing Systems (UCS), Datakeskusvirtualisoinnin kulmakivi, Cisco EXPO 2009, 8.9.2009 Messukeskus, Cisco
[5] Lauri Toropainen, Cisco Maksimoi hyötysi datakeskuksen virtualisoinnin Ciscon ja sen teknologiakumppaneiden avulla, Cisco Expo 2009, 8.9.2009 Messukeskus, Cisco
[6] Harri Ruoho, Dynamic Infrastructure – Role of Datacenter Networking, Cisco Expo 2009, 8.9.2009 Messukeskus, IBM
[7] Olli Kinnunen, Kannattaako virtualisoida ja miksi? Virtualisoinnilla lisää tehoja, kustannussäästöjä ja käytettävyyttä, Cisco Expo 2009, 8.9.2009 Messukeskus, ATEA Finland
[8] Roger Karlsson, Virtualization Beyond the Datacenter, A Holistic Approach, Cisco Expo 2009, 8.9.2009 Messukeskus, Accenture
[9] Stuard Taylor, WAN Optimization: An Accenture point of view on optimization data centers trough application acceleration, Cisco Expo 2009, 8.9.2009 Messukeskus, Accenture
[10] www.ecplaza.net/search/0s1nf20sell/water_source_pump.html
[11] www.cooling.en.alibaba.com
[12] www.google.com/Top/World/Suomi/Tietotekniikka/Internet/kaupalliset_palvelut/Web-hotelllit
[13] itbtlabs.com/articles/peltiercoolers.
[14] www.pa.msu.edu/cmp/csc/nanotube.html
[15] IEEE Spectrum: Silicon Nanowires Turn Heat to Electricity
[16] www.forbes.com/2009/04/07/heat-army-energy-tchnologybreakthroughs-heat.hmtl

APPENDIX 2.

The energy efficiency of Communication networks

Aarne Hummelholm, Technical Manager
Ministry of Finance
Helsinki, Finland
aarne.hummelholm@elisanet.fi,

ABSTRACT

The purpose of this presentation is to describe the situation concerning energy consumption of telecommunications networks according to the current situation, as well as to present alternative solutions to more efficient future telecommunications network systems when it comes to energy consumption.

The presentation provides several possibilities for reducing energy consumption with different solutions involved in and influencing the physical infrastructure of telecommunications networks as well as solutions concerning the actual architectural issues and technical issues of the hardware.

The goal is to create an image of future telecommunications networks solutions, which enable optimization of energy consumption and yet an effective operation of telecommunications environments for producing services in secured operations environments.

This presentation is focusing more ideas than exact calculations of savings. Accurate savings are very difficult to calculate, because equipments new investments values after five to ten years is very difficult to guess right.

INTRODUCTION

The range of the teleservices people need every day grows constantly, and the operational environments needed by the service providers grow along with it, if not even faster. In today's world, people want teleservices where ever they go, even as a real-time service, no matter the costs.

People want to connect to the Internet whenever they want, read their e-mails anywhere, listen to music whenever they feel like it, and watch movies from their computer, regardless of time and place. New social services have made people even more dependent on computers, information technology and the services it provides. They play different kinds of computer games via the Internet or spend time in Facebook telling about their day to others. It is possible to live in a virtual world, when you have time and desire to escape from reality.

People have become addicted to information technology. IT (Information Technology) changes people's operational environments, people themselves, and service supply. In addition, it provides opportunities to operate in a new way and frees time for oneself and one's hobbies.

In the commercial world, electronic commerce, banking and stock market also grows faster than ever.

In the corporate world, people want to simulate different kinds of things, verify the functionality of systems before implementation, model things with 3D (Three Dimensions) models and produce different products with moving pictures for commercials, for instance for the Internet starting page. There are an infinite number of different kinds of service forms, which need more network and server resources in order to work. In addition, service producers constantly try to come up with new appealing services, so that they would gain better results and, thus, develop their own operations.

All of the above means additional requirements in the telecommunications networks increased need of telecommunications capacity as well as an increased need of equipments.

THE CHALLENGES OF TELECOMMUNICATIONS

Different services of information technology and the powerful growth in resulting telecommunications have surprised the telecommunications companies, service producers as well as operators in charge of service environments and data centers.

Within information technology, the operators have not been able to follow and anticipate the development enough, and at the same time optimize all the factors that have an influence on the costs resulting from service production. When offering different kinds of new teleservices to people, no one has considered the aggregate widely enough, and, thus, we have drifted to the current situation – nothing is enough.

different kinds of new teleservices to people, no one has considered the aggregate widely enough, and, thus, we have drifted to the current situation – nothing is enough.

Along with the development and supply of services, the capacity of telecommunications networks has to be constantly increased and new optical cable connections need to be built, in addition to the existing ones. At the same time, the capacity of the technology of transmission networks and data networks is upgraded in size and efficiency also in the rural areas.

The growth in the amount of offered services increases the data centers' hardware base, telecommunications equipments, servers, storage systems, and data security equipments. This, in turn, increases thermal stress.

The thermal stresses of data centers and telecommunications stations are out of control. Their inner spaces are inadequate, recording capacity is insufficient, and delivering the services is not, in all circumstances, flexible and trouble-free. At the same time, the need for energy in data centers increases to such massive amounts that no resources seem to be enough, Image 1.

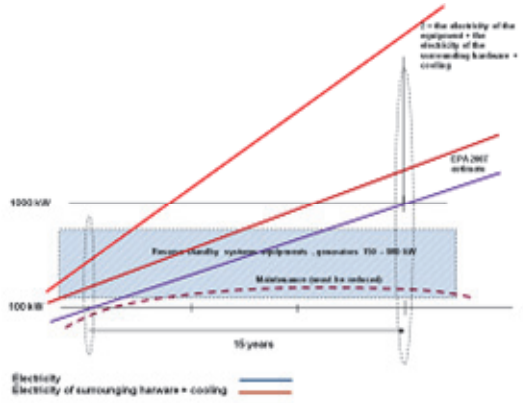


Image 1. The increase prognosis of the energy need of data centers in case no change is made compared to the current situation [1] [2].

As the evaluation of the United States' will EPA (Environmental Protection Agency) shows, the energy requirements of data centers increase about ten-fold during the next 15 years [2]. This is due not just because of fulfilling the energy need of the equipments inside the data centers, but cooling the routers takes up even more electrical energy than the routers themselves. The router manufacturer Cisco predicts an even larger growth. According to their estimate, the energy need of data centers will grow to about 17-fold in the next 15 years [1].
As a result, large data centers need to be built in areas where there is enough energy available even 15 years on from now. One possibility is building an own power plant next to the data centers as, for instance, Google has been forced to do when building new date centers.

Mobile communications services are growth much more faster than ever. This means higher energy needs and thermal stress for thousand communications stations.

Although the energy efficiency of appliances and the components used in them increases, the growth of energy requirements still remains large. In Image 1, this increase in the energy efficiency of components has already been taken into account.

THE DEVELOPMENT OF TELECOMMUNICATIONS

All over the society, the huge rise in energy consumption (Image 1) has brought forth new ideas for reducing energy consumption and making it more efficient. This is called 'Green IT'.

Green IT contains the reduction of energy consumption and energy saving, observation of the carbon footprint in all operations, and reduction of the amount of emissions. It contains new operational models, which are meant to influence people's behavior and consumer habits in order to reduce greenhouse emissions and save energy.

These values are the central concepts of Green IT when planning new data centers spaces, telecommunications stations and restoring the old ones to fulfill new requirements.

Even if we took the Green IT values into consideration when building data centers, we would still fall short of the objectives already in the acquisition stage. Competition legislation does not pay any attention to ecological values.

The equipment systems of the current data centers have still, in part, been built from individual network components, individual servers and server groups as well as storage systems. Each system still has its own control and monitoring equipment with its own monitoring personnel.

Individual equipment instances consume a lot of energy and are, in terms of both control and monitoring, demanding systems which require high expertise.

In addition, the energy consumption is not measured accurately enough, so the realization of energy savings is not properly brought out.

PROFILING OF THE TELECOMMUNICATIONS NETWORKS

Telecommunications networks can also be profiled according to use, as illustrated in Image 2. The need for using telecommunications network connections decreases at during time, so their energy need is also decreased.

However, today all telecommunications networks consume a maximal amount of electrical energy regardless of the situation and loading. Currently, the systems do not have energy saving measures, which would automatically adjust according to the loading and utilization rate.

The first hardware containing energy saving features will probably be introduced into telecommunications networks during 2011.

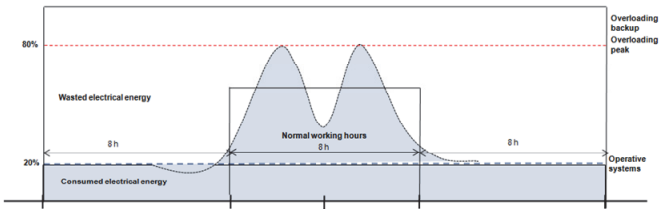


Image 2. The distribution of services during the day.

For instance, if it is assured that a network operator has 100 modern routers (L3-level, OSI models level) in use in the data network, and each P- (Provider router) and PE-router (Provider edge router) uses, on average, 3,000W of electrical energy, the momentary consumption is thus in total 300kW.

On the grounds of Image 3, the indicative energy saving potential of the data network can be calculated in the network of the network operator in question. As an assumption, the energy need of the routers is decreased to 500W/router during the night.

This amounts to energy savings in a day ∑ = 2,500W x 16h = 40,000Wh/day/router
Energy savings in a week ∑ = 40kWh/day x 5 days + (2.5kW x 48h) = 320kWh/week/router
Energy savings in a year ∑ = 320kWh/week x 52 = 16,640kWh/year/router
Financial savings in a year ∑ = 16,640kWh/year x €100/MWh = €1,664/year/router
Financial savings in five years ∑ = €1,664/year x 5 = €8,320 / 5 years / router
Financial savings in five years, 100 routers ∑ = €8,320 / 5 years / router x 100 routers = €832,000 / 5 years (100 routers)

In the future, the energy consumption of telecommunications networks can perhaps be reduced even more than assumed above. The possible contribution of transfer networks has not been observed in the calculations, or the reduction of necessary cooling energy. In addition, in reality the using time of data networks during a day varies according to people's needs, for instance, the utilization rate of the Internet varies. This changes to daily profile of the data network considerably, and, in reality, it does not wholly correspond to the profile of working in an office environment.

PROFILING OF THE WIRELESS NETWORKS

In profiling wireless networks, a use distribution in accordance with Image 3 can also be utilized. The use of wireless networks also decreases during night time, but there is no more specific research available on what the actual utilization rate is and how it is distributed in relation to the networks.

With wireless networks GSM (Global System for Mobile Communications) , 3G (Third Generation Mobile Communications), 4G (Fourth Generation Mobile Communications), LTE (Long Term Evolution), the energy consumption grows on a mean-squared basis when moving from GSM networks to more modern network techniques which provide broadband services, such as 3G and 4G.

An example calculation:

Let us assume that a network operator has 2,000 GSM base stations with the necessary connections in its network. If the network operator would renew its network into 3G, the operator would then need 4,000 base stations to achieve the same radio coverage as in the old 2G network. If the operator would renew its network to 4G, it would take four times more or 16,000 base stations to achieve the same radio coverage. The energy consumption of the network operator's wireless network grows in proportion.

An example calculation:

The input power of a GSM base station from the network is on average 650W
The input power of a 3G base station from the network is on average 300W
The input power of a 4G base station from the network is on average 1000W

The GSM network of the network operator consumes electricity 1,300,000W
Daily consumption of the GSM network is 31,200kWh/day
Annual consumption of the GSM network is thus 11,388,000kWh/year
Annual cost of the energy used by the GSM network is ∑ = 11,388MWh/year x €100/MWh = €1,138,800/year
Financial cost in five years ∑ = €1,138,800/year x 5 = €5,694,000 / 5 years

Respectively, 3G network consumes electricity 1,200,000W
Daily consumption of a 3G network is 28,800kWh/day
Annual consumption of a 3G network is thus 10,512,000kWh/year
The annual cost of the energy used by a 3G network is ∑ = 10,512MWh/year x €100/MWh = €1,051,200/year
Financial cost in five years ∑ = €1,051,200/year x 5 = €5,256,000 / 5 years

4G network consumes electricity 16.000.000 W (16.000 base stations)
Daily consumption of a 4G network is 384 MWh/day

Annual consumption of a 4G network is thus 140.160 MWh/year
Annual cost of the energy used by a 4G network ∑= 140.160 MWh/v x 100 €/MWh = 14.016.000 €/year
Financial cost in five years ∑= 14.016.000 €/year x 5 = 70.080.000 €/5 years

By profiling wireless networks, for instance, with a ratio of 40% / 60%, we can achieve considerable savings in energy consumption and, therefore, in energy costs. The profiling would be done so that 16 hours of a day, the base stations of the network would be more or less on standby, 40% of the maximal load, and 8 hours of the day, the base stations would work with maximum capacity (model Image 3 of the profile).

With this model, the savings of a GSM network are:
The daily consumption of a GSM network is 31,200kWh/day, from which savings can be, in accordance with the previous model (2,000 base stations), 12,480kWh/day and 4,555,200kWh/year.
Financial savings in energy costs of the GSM network are €455,520/year.
Financial savings in five years ∑ = €455,520/year x 5 = €2,277,600 / 5 years

Examples of the advantages in energy savings and costs savings by profiling of wireless networks.

Wireless networks energy use and savings by profiling	GSM	3G	4G
The input power of the base station, W	650	300	1000
The Base stations quantity	2000	4000	16000
Electricity use of network, kW (max.)	1.300	1.200	16.000
Energy savings (60%) /base station (W)	390	180	600
Energy use, kWh/day	31.200	28.800	384.000
Energy savings (60%), kWh/ day	12.480	11.520	153.600
Energy savings (60%), kWh/ year	4.555.200	4.204.800	56.064.000
Financial energy savings, €/ year	455.520	420.480	5.606.400
Financial energy savings, €/ 5 years	2.277.600	2.104.400	28.032.000

Table 5. Examples of the advantages in energy savings and costs savings by profiling of wireless networks, 8h (100% load) and 16h (40% load), summary table.

Respectively, the savings of a 3G network are:
Daily consumption of a 3G network is 28,800kWh/day, from which savings can be, in accordance with the previous model (4,000 base stations), 11,520kWh/day and 4,204,800kWh/year.
Financial savings in energy costs of the 3G network are thus €420,480/year.
Financial costs in five years ∑ = €420,480/year x 5 = €2,104,400 / 5 years

Daily consumption of a 4G network is 384 MWh/day, from which savings can be, in accordance with the previous model (16,000 base stations), 153,6 MWh/day and 56.064 MWh/year.
Financial savings in energy costs of the 4G network are thus €5.606.400 /year.
Financial costs in five years ∑ = €5.606.400 €/year x 5 = €28.032.000 /5 years.

Examples of the advantages of CO_2 savings by profiling of wireless networks.

Greenhouse gas savings in wireless networks	Energy savings kWh/year	CO_2 savings, Tons
GSM networks	4.555.200	3.606
3G networks	4.204.800	3.329
4G networks	56.064.000	44.383

Table 6. Greenhouse gas savings by profiling of wireless networks, summary table.

Also, allocating frequencies regionally may lead to savings in the number of base stations and, thus, in energy consumption. In rural regions, we could use lower frequencies (< 1,000MHz), in which case the base station density could be considerably lower. Since population density is not big in rural areas, the capacity requirement of wireless networks is not as large as in cities and urban areas.

This would reduce the network operator's building costs, maintenance costs of the network and new investment costs, the need for base station locations and equipment spaces. Services could still be offered to all who need them, regardless of time and space, also as broadband.

The energy use efficiencies of base stations and communications stations of communications networks are under 20%, so the energy efficiency of those stations has to be improved also when it comes to their infrastructure. This way, we would gain savings in costs.

THE DEVELOPMENT OF THE ENERGY SUPPLY OF DATACENTERS, WIRELESS NETWORKS AND TELECOMMUNICATIONS NETWORKS

If we would use direct voltage as the power-supply voltage of data centers, wireless networks and telecommunications networks' hardware, this would erase, among others, the need for UPS in data centers. Using direct voltage also improves the efficiency of energy supply. In the execution, we could leave voltage conversions out of the energy supply system,

which means more efficiency. The efficiency can be improved by over 10% [2] [13] [14] [15] [16].

At the moment, the obstacles in the way of technical development are commercial aspects rather than technical solutions.

We can take a 1MW data centers as an example. When we count the effect of a 10% efficiency improvement value to the energy consumption, the resulting value is 100kW. Although at first glance the sum seems small, the energy savings during the day are as much as 2,400kWh/day.

In a year, this results in energy savings of 876,000kWh/year (an example).

Thus, financial savings on an annual level are €87,600 (€100/MWh).
Financial savings in five years ∑ = €87,600/year x 5 = €438,000 / 5 years

This money can be used in acquiring physical server resources, which can be utilized with the help of virtualization, as previously mentioned in section 3.2. This, in turn, considerably increases the advantages gained from improving the energy supply, when reviewing the matter as a whole. The point comes across well in the previously calculated example.

Let us also count, on the base of the wireless network solutions in section 3.5, the savings attainable for a network operator, when the energy supply is changed to direct voltage.

The GSM network of a network operator consumes electricity 1,300,000W and a 3G network respectively 1,200,000W, which means that the input power is in total 2,500,000W or 2,500kW.
If we can utilize 10% of this consumption with the help of direct voltage from the input power, we get 250kW. During the day, the savings in electricity consumption are then 6,000kWh/day.
Therefore, the amount of saved energy during the year is 2,190,000kWh/year.
Financial savings on an annual level are thus €219,000/year (€100/MWh).
Financial savings in five years ∑ = €219,000/year x 5 = €1,095,000 / 5 years

The same technique can be applied in the energy supply systems of the communications stations of telecommunications networks. The number of communications stations in the telecommunications networks often also arises to thousands, so the energy saving potential in the systems of the network operator is considerable as a whole.
The direct voltage system can also be executed as a hybrid solution, in which case solar power, energy cells (previous fuel cell technique), biofuel systems, wind power and other renewable energy forms can be integrated into it. This entity will reduce dependency from imported fuels and, at the same time, the energy supply systems will be considerably more reliable than they currently are.
When adding up the advantages of profiling and energy supply, we can achieve considerable savings in energy and costs. Cost efficiency can also be increased by building more efficient communications stations in regard to energy consumption. Often the communications station buildings leak their thermal energy straight outdoors, their door and windo
structures are simple and the heat energy escapes. These issues have not been taken into consideration in the calculations.

Examples of the advantages in energy savings and costs savings by the development of the energy supply of data centers and wireless networks.

Energy savings by development of the energy supply	GSM	3G	4G
The input power of the base station, W	650	300	1000
The Base stations quantity	2000	4000	16000
Electricity use of network, kW (max.)	1.300	1.200	16.000
Energy savings, W	390	180	600
Energy use, kWh/day)	31.200	28.800	384.000
Energy savings (10%), kWh/day	3.120	2.880	38.400
Energy savings (10%), kWh/year	1.138.800	1.051.200	14.016.000
Financial energy savings, €/year	113.880	105.120	1.401.600
Financial energy savings, €/5 years	569.400	525.600	7.008.000

Table 7. Examples of the advantages in energy savings and costs savings by the development of the energy supply of wireless networks (DC-systems, direct voltage systems), summary table.

Greenhouse gas savings in wireless networks	Energy savings kWh/year	CO_2 savings, Tons
GSM networks	4.555.200	3.606
3G networks	4.204.800	3.329
4G networks	56.064.000	44.383

Table 6. Greenhouse gas savings by profiling of wireless networks, summary table.

TRANSFORMING WASTE ENERGY INTO COOLING ENERGY AND ELECTRICITY

A completely new idea in reducing the energy consumption of data centers is the possibility of utilizing the waste heat of data centers in cooling them. The innovation is based purely on classic physics. Image 4 shows the influence of this in the total energy consumption of data centers.

Data centers produce large amounts of thermal energy which goes to waste. Utilizing and recycling this wasted energy would reduce the energy need, use costs and also the renewal need of the surrounding hardware of data centers.

Preliminary research shows that more than 70% of the waste heat could be utilized by changing it back to cooling energy. Even this result is better than not utilizing the waste heat at all. The aim is to reduce the need of intake energy of data centers, and, thus, lower the costs as well as the need for electrical energy.
This is also of great significance internationally, if the waste heat of each data centers can be utilized by even over 70% efficiency and, in addition, the energy need of data centers cut down during the night. Previously, households could use by night time electricity, which was cheaper than daytime electricity. This solution also leveled the electricity consumption during the day. We should only find the right ratio between the use of night time and daytime electricity [10] [11].

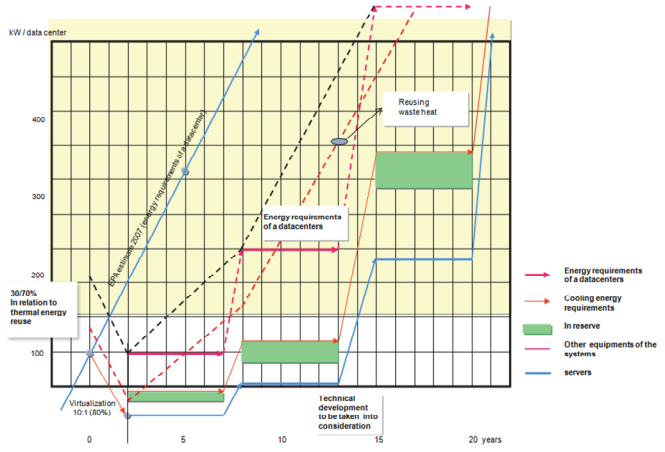


Image 4. An example of energy savings attained by reusing the wasted thermal energy of data centers.

If we assume that a country has, for example, 20 data centers of 1MW, then they need 20MW for the energy of the hardware alone. If we then calculate the amount of energy required by the data centers and the surrounding hardware, the energy need is approximately 40MW [2], of which the portion of the cooling energy is about 20MW.

If we can utilize 70% of the waste heat produced by a data center, we can utilize 14MW of the cooling energy of 20MW again as cooling energy. At the same time, we can reduce the amount of input power of the data centers and gain savings in costs.

As an example, we can calculate what this means in terms of expenses.

20MW of energy means during the day 480MWh/day.
On an annual level, the energy consumption is 175,200MWh/year.
If we can reuse 70% of this amount of energy, it means 122,640MWh.
The cost of the reusable energy is €12,640,000/year.
Financial cost in five years ∑ = €12,640,000/year x 5 = €63,200,000 / 5 years

In the calculations, it has been assumed that building the data centers is done with the principles according to Image 2.

The obtained result can be examined in accordance with Image 1 for the whole period of 15 years. In the image, the energy consumption increases 10-fold during a period of 15 years. When we do not take index increases into account, the financial cost of the previously calculated sum for 15 years will be €189,600,000 / 15 years, calculated merely on the basis of the starting situation.

But energy consumption has increased after five years and, during that time, has already doubled, so the need for cooling energy has also doubled. The same applies for the next period of five years, when the consumption is three times the starting value.

Calculated on this basis, the financial cost of the reusable energy during the next period of five years is ∑ = €63,200,000 / 5 years x 2 =€126,400,000 / 5 years.

Respectively, the cost of reusable energy for the next period of five years is ∑ = €126,400,000 / 5 years x 3 = €379,200,000 / 5 years.

The financial cost of the reusable energy for the whole period of 15 years is €568,800,000 / 15 years calculated according to the values of images 2 and 4. Even if the virtualization of data centers would be executed in accordance with Image 2, we would still need cooling energy.

Costs in savings are enormous. At the moment, there are already 52 web data centers in Finland [12]. When we add the data centers owned by organizations to this, reusing even this waste heat and with these efficiencies we will gain enormous savings on an annual basis. It is difficult to find out more specific numbers of data centers.
New type of integrated cooling, heating and power systems payback is about 3 to 5 years.

purely on classic physics. This solution has not yet been applied to data centers. The technique has been developed, among others, to satisfy the energy needs of space ships.
This solution can further improve the energy efficiency of data centers, by utilizing the remaining waste heat and transforming it directly to electrical energy.

Transforming waste heat into electrical energy can, at present, be done with the help of Peltier elements, but the efficiency is not very high [13].
Better solutions are sought from the applications of nanotechnology, means of which waste heat can directly be transformed into electrical energy. Nano pipes are one of the most promising transforming elements in this model [14. In addition, nanowire seems to be another efficient energy transformer of the future for transforming heat energy directly into electricity [15].

In the United States, the army is exploring the possibility of utilizing the heat energy of exhaust pipes of heavy trucks in recharging batteries. Technical solutions are available and they can be directly utilized in transforming heat energy into electricity. These solutions have not yet been applied to data centers environments [16].

In both alternatives, the acquisition costs and life cycle costs of the techniques need to be considered in order to calculate the eventual benefit.

Transforming waste energy into electricity is done with passive components, which have a long life cycle (~ over 30 years).

Examples of the advantages in energy savings and costs savings by transforming waste energy into cooling energy of data centers, summary

Reusing the wasted thermal energy	Data centers
Electrical energy use for cooling, kW (max)	20.000
Cooling energy use, kWh/day	480.000
Cooling energy use, kWh/ year	175.200.000
The wasted termal energy reusing (70 %), kWh/ year	122.640.000
Thermal energy reusings financial savings, €/ year	12.264.000
Thermal energy reusings financial savings, €/ 5 years	61.320.000
Thermal energy reusings financial savings, €/ 15 years , (Image 4)	551.880.000

Table 6. Example of energy savings attained by reusing the wasted thermal energy of data centers (70 % reuse), summary table.

ENERGY EFFICIENCY OF DATA CENTERS AND TELECOMMUNICATION STATIONS

The energy efficiency of data center is a criterion, which is used to define the performance of a data center. The energy efficiency of a data center is defined with DCiE value (DCiE = Data Centre infrastructure Efficiency). The DCiE value is the relation between the power of the IT equipment and the overall power of the data centers [7] [8]. With this value, we can compare the energy efficiency of different data centers very precisely. Therefore, energy measuring systems need to be designed into the data centers, so that the DCiE value can be properly measured. Another term used in measuring energy efficiencies is PUE (PUE = Power Usage Effectiveness). DCiE is 1/PUE.

With the help of DCiE (PUE) definitions, we can also measure the energy efficiencies of telecommunication stations and base stations of a wireless network. In these telecommunication stations of a telecommunications network, the energy efficiency is currently considerably less than 20%, so by using a common measuring method, we can compare the energy efficiencies and also improve the efficiency of the energy use of telecommunication stations of telecommunications networks. This method has not been commonly used in measuring the energy efficiencies of telecommunications networks.

CONCLUSION

In data centers, communication stations of telecommunications networks and base stations of wireless networks, there are a lot of above-mentioned improvements that can be made in regard to energy saving.

Some of the presented savings models are wholly new solutions, which have not yet been applied, at least on a larger scale, in Finland for data centers, communications stations of telecommunications networks or base stations of wireless networks.

European countries can also save tens or even hundreds of millions of Euros in a year with these solutions. In addition, and telecommunications networks are not the only places, which form waste heat that is not utilized at all, but these also include, for instance, factories, oil refineries, power plants as well as all structures that produce heat.

Even with all the talk in the world of recycling and reusing materials as well as collecting paper, carton, metal, glass and equipment scraps for reuse, still the recovery of waste heat is minimal.

However, there are enormous savings to be made in reusing waste heat, in Finland and in other countries, as well. The financial savings are tremendous. If we can implement the

presented energy saving possibilities, even in part, we can also save immense amounts of funds in building power plants and other energy producing institutions as well as in carbon footprints nationally and worldwide.

The electrical energy of ITC systems and equipment is only a few per cents of the overall consumption of electrical energy in the world. We can only roughly estimate the overall amount of produced waste heat in the world, and this goes directly to the atmosphere to heat the air. The amount of energy in the waste heat can be billions of kilowatt-hours for every use hours worldwide. No matter how clean the waste heat is, it still heats the atmosphere. Just like pollution is carried with air currents from one place to another, so does this waste heat, by warming the atmosphere. Where and how this waste heat released into the atmosphere can dissolve, so it would not heat the Earth's atmosphere? According to the law of indestructibility of energy it goes as a whole to some place, where it does not necessarily belong to, and causes its own addition to the warming of the atmosphere.

What are the climatic influences of waste heat directly released into the air? This cannot even be estimated without extensive research.

What we can do for energy savings now and the future are that we start to design whole infrastructure of society taking care of energy saving possibilities, recycling and reusing wasted thermal energy, optimise and profile communications networks, communications stations and data centers.

SOURCES:

[1] Jan Linström, Data Center present and Future Directions, Cisco
[2] Reijo Mäihäniemi, CEO and President of Efore, ICT Getting Green, Efore, 14.10.2008
[3] Keijo Niemistö, Ympäristöystävällinen IT, TTL 3.4.2008, VMware - Energian säästöä palvelinten virtualisoinnilla, VMware Finland
[4] Tomi Jalonen, Cisco Unified Computing Systems (UCS), Datakeskusvirtualisoinnin kulmakivi, Cisco EXPO 2009, 8.9.2009 Messukeskus, Cisco
[5] Lauri Toropainen, Cisco Maksimoi hyötysi datakeskuksen virtualisoinnin Ciscon ja sen teknologiakumppaneiden avulla, Cisco Expo 2009, 8.9.2009 Messukeskus, Cisco
[6] Harri Ruoho, Dynamic Infrastructure – Role of Datacenter Networking, Cisco Expo 2009, 8.9.2009 Messukeskus, IBM
[7] Olli Kinnunen, Kannattaako virtualisoida ja miksi? Virtualisoinnilla lisää tehoja, kustannussäästöjä ja käytettävyyttä, Cisco Expo 2009, 8.9.2009 Messukeskus, ATEA Finland
[8] Roger Karlsson, Virtualization Beyond the Datacenter, A Holistic Approach, Cisco Expo 2009, 8.9.2009 Messukeskus, Accenture
[9] Stuard Taylor, WAN Optimization: An Accenture point of view on optimization data centers trough application acceleration, Cisco Expo 2009, 8.9.2009 Messukeskus, Accenture
[10] www.ecplaza.net/search/0s1nf20sell/water_source_pump.html
[11] www.cooling.en.alibaba.com
[12] www.google.com/Top/World/Suomi/Tietotekniikka/Internet/kaupalliset_palvelut/Web-hotelllit
[13] itbtlabs.com/articles/peltiercoolers.
[14] www.pa.msu.edu/cmp/csc/nanotube.html
[15] IEEE Spectrum: Silicon Nanowires Turn Heat to Electricity
[16] www.forbes.com/2009/04/07/heat-army-energy-tchnologybreakthroughs-heat.hmtl