JYU DISSERTATIONS 409

Tiina Kovanen

Cyber-Threat Aspects in a Complex System-of-Systems Environment

A Case Study in Remote Pilotage

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 409

Tiina Kovanen

Cyber-Threat Aspects in a Complex System-of-Systems Environment

A Case Study in Remote Pilotage

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi
syyskuun 3. päivänä 2021 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
on September 3, 2021, at 12 o'clock.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2021

Editors
Timo Männikkö
Faculty of Information Technology,, University of Jyväskylä
Päivi Vuorio
Open Science Centre, University of Jyväskylä

Copyright © 2021, by University of Jyväskylä

ISBN 978-951-39-8771-8 (PDF)
URN:ISBN:978-951-39-8771-8
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-8771-8

ABSTRACT

Kovanen, Tiina
Cyber-threat aspects in a complex system-of-systems environment: A case study in remote pilotage
Jyväskylä: University of Jyväskylä, 2021, 62 p. (+ articles)
(JYU Dissertations
ISSN 2489-9003; 409)
ISBN 978-951-39-8771-8 (PDF)

Society's vital functions depend on critical infrastructure which covers many elements, from energy production to transportation of goods. This environment is transforming toward an automated and digitalized future. This future creates new information technology environments and networked systems that may include legacy components that were not designed to function securely outside an isolated environment. Furthermore, the dependency between separate systems creates a system of systems that are more complex to design.

The development of a digitalized operation of systems will decrease the risk of human error, as decisions are either made by the systems themselves or a human operator receives guidance and alerts. However, removal of the human element introduces new types of threats when, for example, human vision is removed from sensing the operational surroundings. This may delay detection of malfunctions if the corresponding digital sensor is not deployed. Accidents and malfunctions are examples of events that occur incidentally. However, a digitalized environment increases the risk of deliberate malicious cyber-attacks. Therefore, to protect these new environments, understanding the cyber threats and actors is vital.

This dissertation discusses this type of development and presents a remote pilotage environment, ePilotage, as a case study in which cyber threats are examined. The research produces a description of the threat actor and scenarios that may be used with the design process and development of the ePilotage environment. As maritime transportation and ports are considered part of the European critical infrastructure, this case study provides knowledge for other critical infrastructures that are transforming from traditional engineering environments to interconnected versions.

Keywords: critical infrastructure, maritime autonomy solution, ePilotage, cyber threat, cybersecurity

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Kovanen, Tiina
Kyberuhka monimutkaisessa järjestelmien järjestelmässä - tapaustutkimus etäluotsausympäristössä
Jyväskylä: University of Jyväskylä, 2021, 62 s. (+artikkelit)
(JYU Dissertations
ISSN 2489-9003; 409)
ISBN 978-951-39-8771-8 (PDF)

Yhteiskunnan elintärkeät toiminnot riippuvat kriittisen infrastruktuurin toimivuudesta. Tähän kuuluvat muun muassa energian tuotanto ja erilaisten hyödykkeiden toimitusketjut mukaan lukien meriliikenne ja satamat. Nämä ympäristöt ovat mukana muutoksessa kohti digitaalisempaa ja verkottuneempaa tulevaisuutta. Muutoksen johdosta syntyy uusia tietoteknisiä verkottuneita ympäristöjä, joissa voi olla mukana jäänteitä vanhoista toimintaympäristöistä. Tällaiset vanhat järjestelmät eivät välttämättä toimi turvallisesti verkottuneessa ympäristössä, jos niiden suunnittelussa ei sitä aikoinaan ole otettu huomioon. Lisäksi erillisten ympäristöjen verkottuminen keskenään luo järjestelmien järjestelmän, joka lisää monimutkaisuutta suunnittelutyöhön.

Digitaalisemmat ympäristöt ja järjestelmät pienentävät inhimillisen virheen mahdollisuutta, koska ihminen voidaan joko poistaa päätöksentekoprosessista tai avustaa päätöksen tekoa informaatiolla ja hälytyksillä. Ihmiselementin poisto poistaa kuitenkin myös havainnontekomahdollisuuksia, kun ei voida nähdä tilanteita tapahtumapaikalla. Tämä voi johtaa toimintahäiriöiden havaitsemisen viivästymiseen, ellei havainnon korvaavaa sensoria ole asetettu. Onnettomuudet ja toimintahäiriöt ovat esimerkkejä tahattomista tapahtumista. Digitaalisemmat ympäristöt kuitenkin lisäävät myös tahallisten kyberhäiriöiden riskiä. Tämän vuoksi kyberuhkan ja kybertoimijoiden ymmärtäminen on olennainen osa näiden uusien järjestelmien turvaamisen mahdollistamisessa.

Tämä väitös käsittelee tätä muutosta ja esittää etäluotsausympäristön, ePilotagen, tapaustutkimuksena. Tutkimus tuottaa kuvauksen kyberuhkasta ja skenaarioita kyberuhkatoiminnasta etäluotsausympäristössä. Näitä voidaan hyödyntää ePilotage-ympäristön suunnittelu- ja kehitystyössä. Koska meriliikenne ja satamien toiminta on määritelty kuuluvaksi Euroopan Kriittiseen Infrastruktuuriin, tuottaa tapaustutkimus myös tietoa muille kriittisen infrastruktuurin alueille, joissa ollaan siirtymässä kohti etätoimintoja ja automaatiota.

Avainsanat: kriittinen infrastruktuuri, meriliikenteen automaatio, ePilotage, kyberuhka, kyberturvallisuus

Author

Tiina Kovanen
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors

Professor Timo Hämäläinen
Faculty of Information Technology
University of Jyväskylä
Finland

Professor Pekka Neittaanmäki
Faculty of Information Technology
University of Jyväskylä
Finland

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

Reviewers

Professor Kirsi Helkala
Norwegian Defence Cyber Academy
Norway

Professor Rauno Kuusisto
Finnish Defence Research Agency
Finland

Opponent

Principal lecturer, Docent Rauno Pirinen
Laurea University of Applied Sciences
Finland

ACKNOWLEDGEMENTS

This thesis is based on the work done at the University of Jyväskylä's faculty of Information Technology. During the years I have had the privilege to participate in many research projects and gained academic insight into various topics mostly concerning cyber security of critical infrastructures or cyber-physical systems. For the thesis, the main case studied is the remote pilotage environment ePilotage, which combines the previously studied topics.

I wish to thank my supervisors professors Timo Hämäläinen, Pekka Neittaanmäki and Martti Lehto for research opportunities and support while the research was ongoing. I also wish to extend my gratitude to Gil David who act as my supervisor at the beginning of my PhD work.

Furthermore, special thanks go to my reviewers professors Kirsi Helkala and Rauno Kuusisto and to my opponent docent Rauno Pirinen. Their viewpoints helped to clarify my text and offered food for though. Their comments are highly appreciated and helped to improve my thesis.

Finally, this would have not been possible without the love and support from my family. I wish to thank my sons Santeri and Viljami for their patience during the writing process and my husband Mika for the encouragement while finishing this thesis seemed to be unachievable.

Jyväskylä 29.7.2021
Tiina Kovanen

ABBREVIATIONS

AIS	Automatic Identification System
AtoN	Aid to navigation
ATT&CK®	Adversary tactics and techniques
ARPA	Automatic radar plotting aid
CI	Critical infrastructure
CIA	Confidentiality, Integrity, Availability
CII	Critical information infrastructure
CIP	Critical Infrastructure Protection
CKC	Cyber kill chain
CPS	Cyber-physical system
DoS	Denial of Service
DSC	Distributed control systems
ECDIS	Electronic Chart Display and Information System
ECI	European critical infrastructure
EPCIP	European Programme for Critical Infrastructure Protection
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HMI	Human–machine interface
ICS	Industrial control system
ICT	Information and communication technology
IMO	International Maritime Organization
IOC	Indicator of compromise
ITU	The International Telecommunication Union
IDS	Intrusion detection system
MMSI	Maritime Mobile Service Identity
MSMS	Maritime Security Management System
NIST	National Institute of Standards and Technology
SCADA	Supervisory Control And Data Acquisition
SoS	System of systems
VHF	Very-High-Frequency (radio wave)
VTS	Vessel traffic service

FIGURES

TABLES

CONTENTS

LIST OF PUBLICATIONS

This dissertation is based on seven publications.

PI Kovanen, T., David, G., & Hämäläinen, T. (2016). Survey: Intrusion detection systems in encrypted traffic. In O. Galinina, S. Balandin, & Y. Koucheryavy (Eds.), *Internet of Things, Smart Spaces, and Next Generation Networks and Systems* (pp. 281–293). Springer International Publishing.

PII Kovanen, T., Nuojua, V., & Lehto, M. (2018). Cyber threat landscape in energy sector. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (pp. 353-361), Washington DC, USA. Academic Conferences and Publishing Limited.

PIII Kemppainen, S., & Kovanen, T. (2018). Honeypot utilization for network intrusion detection. In *Cyber Security: Power and Technology* (pp. 249-270). Cham: Springer.

PIV Pöyhönen, J., Kovanen, T., & Lehto, M. (2021). Basic elements of cyber security for an automated remote piloting fairway system. In *ICCWS21 16th International Conference on Cyber Warfare and Security*, Tennessee, USA. Academic Conferences International Limited.

PV Kovanen, T., Pöyhönen, J., & Lehto, M. (2021). ePilotage system of systems' cyber threat impact evaluation. In *ICCWS21 16th International Conference on Cyber Warfare and Security*, Tennessee, USA. Academic Conferences International Limited.

PVI Hummelholm, A., Pöyhönen, J., Kovanen, T., & Lehto, M. (2021). Cyber security analysis for ships in remote pilotage environment. In *ECCWS21 20th European Conference on Cyber Warfare and Security*, Chester, UK.

PVII Kovanen, T., Pöyhönen, J., & Lehto, M., (2021). Cyber threat analysis in the remote pilotage system. In *ECCWS21 20th European Conference on Cyber Warfare and Security*, Chester, UK.

Papers PI, PII, and PIV–PVII were published in Jufo 1 classified conferences.
PIII was published in a Jufo 2 classified monograph.

THE AUTHOR'S CONTRIBUTION TO THE ARTICLES

The author had the main research and writing responsibility for the publications of which she is the first author. For publication PIII, the author focused on the final writing process, interpreting the results and the context surrounding the honeypot experiment. For publications PIV and PVI, the author participated in the research project, communicated about the topic, and made a minor contribution to writing the publications.

Publications PI through PIII were written while the author was a project researcher at the University of Jyväskylä. Publications PIV through PVII were written when the author was a PhD student at the University of Jyväskylä for the Sea for Value (S4V) project and not employed by the university. This thesis was written with a two-month grant from the University of Jyväskylä.

1 INTRODUCTION

1.1 Research motivation

Maritime transportation and ports are identified as parts of European critical infrastructure (ECI), and their disruption or destruction would have a significant impact on society's vital functions in European Union member states (Council of the European Union, 2008). The DIMECC program Sea for Value – Fairway brings together research organizations, industrial partners, and government authorities to improve safe navigation to and from ports for current vessels and to prepare for the arrival of autonomous vessels (DIMECC, 2020). Remote pilotage, ePilotage, is part of this package. This thesis provides knowledge of cyber threats to this environment.

Understanding the cyber adversary's motivation and attack techniques is a proactive approach that enables designers to allocate their resources more effectively (Casey, 2015). This is the aspect that this research offers. The ePilotage is in the design phase and therefore detailed information on the technological aspects does not exist. On the general level the environment has unique features, such as cyber-physical systems (CPSs). Industrial control systems (ICSs) and various sensors are used in the CPS setting more than in traditional information and communication technology (ICT) environments. Therefore, existing cyber-threat models designed for pure ICT environments are not ideal for ePilotage.

In this thesis, system analysis is conducted by examining system components affecting cybersecurity, potential impacts of cyber-attacks, and case studies from specific critical points (such as ships) and near-field areas (such as the energy sector). Actors and motivations are also investigated. Finally, attack scenarios in the ePilotage environment are constructed. This offers a comprehensive knowledge base for the system design process and a starting point for system defense. For other industrial fields, this thesis offers a case study of cyber threats against an environment that is transitioning from traditional engineering solutions to an automated future.

The aim of this study is two-fold. It examines cybersecurity as a systems-related phenomenon but combines it with practical frameworks used by the cybersecurity industry. The purpose is to provide usable information for system development with academic research results.

Publications PI through PVII examines these themes, and the links are presented in figure 1. Publications PI and PIII examine cyber threats and their detection. Publication PII surveys actual attacks against critical infrastructure in the energy sector. Publication PIV presents the ePilotage environment and cybersecurity constructs. Publications PV through PVII discuss cyber threats in the ePilotage system environment.

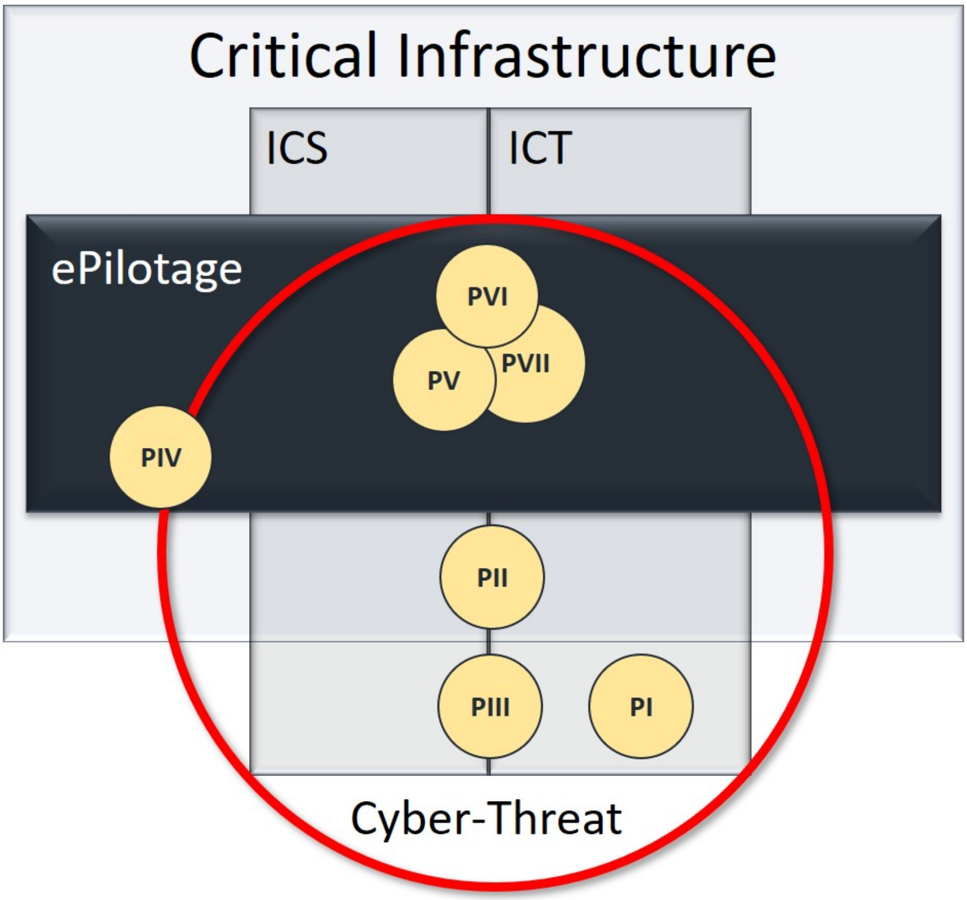


FIGURE 1 Thesis publications presented in the context of the related themes.

1.2 Research objectives and research questions

ePilotage is a new type of environment, and thus, examining cyber threats in that environment is impossible. Therefore, to understand the phenomenon, the research objectives include investigating cyber-attacks and their detection at a general level. The other research questions are directly related to the ePilotage environment and use knowledge from previous studies.

1.2.1 Examination and detection of cyber threats

RQ1: What type of cyber-attacks have occurred in critical infrastructure? (PII)
RQ2: How does increased encryption affect detection of attacks? (PI)
RQ3: What type of attacks are detected with honeypots? (PIII)

1.2.2 ePilotage environment and cyber threats

RQ4: What does the ePilotage environment consist of? (PIV)
RQ5: What are the cybersecurity elements of ePilotage? (PIV)
RQ6: What are the impacts of cyber-attacks in ePilotage? (PV)
RQ7: How to estimate cyber risk in the complex modern ship environment? (PVI)
RQ8: What are the characteristics of cyber threats to ePilotage? (PVII)
RQ9: How to create cyber-attack scenarios for ePilotage? (PVII)

1.3 Research projects related to the thesis

Sea for Value (S4V) Fairways is a DIMECC program aiming to aid maritime digitalization, service innovations, and information flows. The program’s long-term mission is preparing for advanced autonomous operations and navigation. The focus is on fairways, enabling safe passage for ships to and from harbors. The program is facilitated and organized by the DIMECC, funded by companies and Business Finland. Participants include industrial partners, research organizations, and government authorities and association. This thesis was researched and written with the participation of the University of Jyväskylä.

1.4 Outline of the thesis

This thesis is divided into four chapters. Theoretical background information is presented in Chapter 2, and the results section for ePilotage is presented in Chapter 3. The results are discussed in Chapter 4, and answers to the research questions, implications for the practical ePilotage design process, and limitations of the results are offered. Future research directions are also discussed

2 THEORETICAL BASIS OF THE RESEARCH

2.1 Introduction

Enabling automated maritime traffic through advancements in remote pilotage is a highly contemporary topic with direct practical benefits. From a broad perspective, it is a phenomenon in the modern world seen in other similar technological advancements. As the subject is new, limited historical data are available; scientific contributions have just started to accumulate and are either narrowly focused, or similar topics are discussed in different environments. Therefore, background information must be retrieved from multiple different topics.

2.2 Objectives and organization of the chapter

This chapter provides a context for the thesis and places its contributions among related research fields and theoretical frameworks. First, the research approach and data are discussed. Then, relevant background information is presented from the fields of cybersecurity, critical infrastructure, and maritime transportation. Finally, previous and related research is introduced. Publication PII is presented as part of critical infrastructure discussion and research question 1 is answered in chapter 2.7.2.

2.3 Research approach

The constructive research approach is used for this thesis as the aim is to produce a description of cyber threats to a system. This system is the ePilotage environment, which offers a single-case case study in a larger field of complex ICS environments.

The constructive research approach focuses on relevant real-world problems and aims to produce a construction as an innovative solution (Lukka, 2003). In this thesis, the problem arises from the undescribed cyber-threat adversary in the novel ePilotage environment, and the construction is to produce a model of cyber threats based on previous work in multiple separate cybersecurity fields. The practical aspect of this model manifests in its capability to produce justified attack scenarios for development of the system.

A case study is a qualitative approach well suited for addressing contemporary phenomena in the real-life context (Meyer, 2001). The steps for designing a case study include selecting single or multiple cases, the data sampling period, and the data collection procedures (Meyer, 2001). In this thesis, only a single case, the ePilotage environment, is addressed because this is the environment for which the solution is intended.

A case study has advantages for this study but also has disadvantages. One is the challenge of generalizing the results. The limitations are addressed in more detail in Chapter 4 at the end of this thesis.

2.4 Research data

Because the ePilotage environment is still at the concept level, a detailed evaluation of the technical choices and related vulnerabilities cannot be performed. Moreover, the number of published attacks against maritime environments is limited. Therefore, the research utilizes knowledge of near-field cases and databases. These include reports on incidents in other critical infrastructure or ICS environments and databases containing information on cyber-attacks.

Cyber adversary information is gathered from literature consisting of cybersecurity companies' white papers, academic publications, threat databases, and news reports. Because information about fairway systems is scarce, near-field cases are used for reference. These cases include other critical infrastructure, ICS-related incidents, and other maritime cyber threats, especially against ships. The use of non-academic sources is justified because the current practical information is necessary for a realistic model and a requirement for the model to stay up-to-date in the future.

Using varied sources raises the concern of data validity. In particular, the purposes of news reports and companies' public announcements is not necessarily to provide deep and accurate knowledge but to convince business continuity or to gain readers.

2.5 Theoretical framework of the research

The research is part of larger research areas of critical infrastructure (CI), including Critical Infrastructure Protection (CIP) and cyber-physical systems (CPS), Cybersecurity, and Systems study. From the systems research point of view, the tight coupling of multiple complex systems raises concern about natural accidents (Perro, 2001). If we add to this concept the idea of a determined malicious cyber adversary, a cyber-threat study for this environment is one of the key elements for safer fairway navigation. Moreover, ePilotage is an example of the system of systems (SoS) environment, where multiple independent constituent systems work together to fulfill the function of the SoS.

2.6 Cybersecurity

The cyber world consists of many different abstraction levels. Martin Libicki (2007) created a structure for the cyber world based on the Open Systems Interconnection (OSI) reference model which layers communication protocols. Lehto and Neittaanmäki (2018) later enhanced this cyber-world model with an additional service layer. The layers are presented in figure 2. The first layer, physical layer, is the most concrete, and the physical structures form the communication network. The second layer, syntactic layer, controls the data flow and includes, for example, network protocols. The third layer, semantic layer, consists of data, and in the case of an ICS, the process control functions. The fourth layer, service layer, enhances Libicki's model by introducing services. This brings this model closer to contemporary ICT environments that consist of more than just the user's own computer environment. The fifth layer, cognitive layer, focuses on the perception of information and contextual understanding.

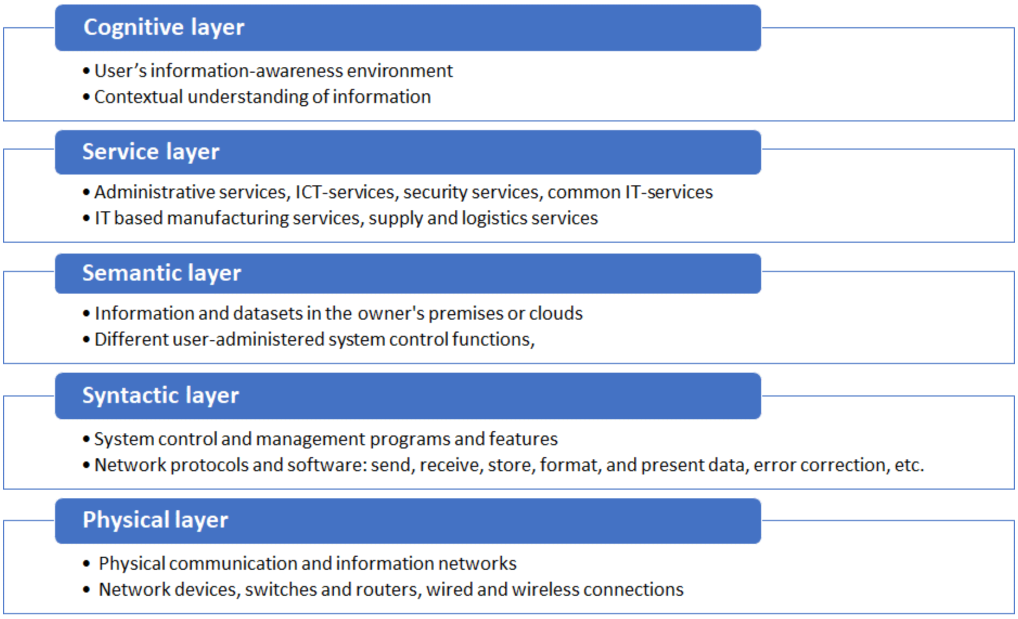

Cognitive layer
• User's information-awareness environment
• Contextual understanding of information
Service layer
• Administrative services, ICT-services, security services, common IT-services
• IT based manufacturing services, supply and logistics services
Semantic layer
• Information and datasets in the owner's premises or clouds
• Different user-administered system control functions,
Syntactic layer
• System control and management programs and features
• Network protocols and software: send, receive, store, format, and present data, error correction, etc.
Physical layer
• Physical communication and information networks
• Network devices, switches and routers, wired and wireless connections

FIGURE 2 The five-layer structure of the cyber world (Lehto & Neittaanmäki, 2018, adapted).

In this cyber world, the definition of cybersecurity is not straightforward. Often, information security is used as a synonym, although cybersecurity can be viewed as encompassing a broader set of targets for attacks (von Solms & van Niekerk, 2013). The International Telecommunication Union (ITU) defines cybersecurity through a collection of means, such as tools, policies, and actions, to protect the cyber environment, organization, and user's assets against relevant security risks in the cyber environment (ITU-T, 2008). The ITU states the general security objectives: Confidentiality, Integrity, and Availability. These objectives are often referred to by the abbreviation CIA. National cybersecurity strategies in different countries have their own definitions of cybersecurity, and there is no common, harmonized definition (Luiijf, Besseling & De Graaf, 2013). In this thesis, the definition used is stated in Finland's cybersecurity strategy (Secretariat of the Security Committee, 2013): "Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured."

Cybersecurity in a large organization or in an SoS must be understood at many different abstraction levels to secure the whole. Combining the five-layer cyber-world model in decision-making levels provides a comprehensive system view of an organization's cybersecurity (Pöyhönen & Lehto, 2020). This model is presented in figure 3.

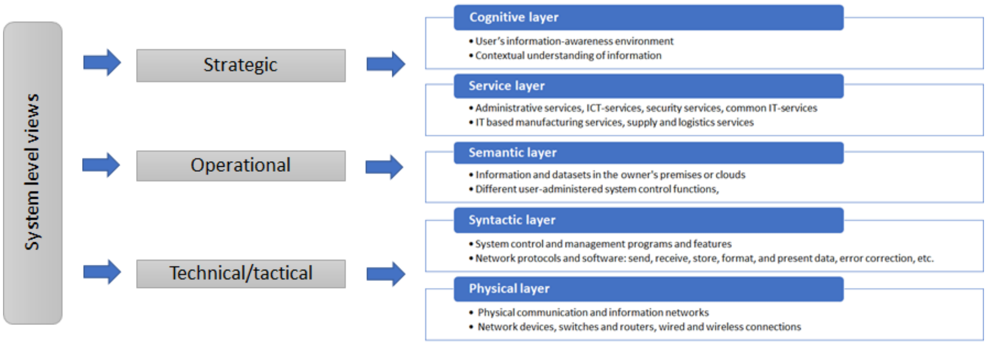

System level views
Strategic
Operational
Technical/tactical
Cognitive layer
• User's information-awareness environment
• Contextual understanding of information
Service layer
• Administrative services, ICT-services, security services, common IT-services
• IT based manufacturing services, supply and logistics services
Semantic layer
• Information and datasets in the owner's premises or clouds
• Different user-administered system control functions,
Syntactic layer
• System control and management programs and features
• Network protocols and software: send, receive, store, format, and present data, error correction, etc.
Physical layer
• Physical communication and information networks
• Network devices, switches and routers, wired and wireless connections

FIGURE 3 Five-layer model combined with the decision-making level for a system-level view on organizational cybersecurity (Pöyhönen & Lehto, 2020).

Cybersecurity is closely related to the notion of cyber risk. Risk is often defined through the probability of an event and its impact. Bimco (2020) ties this definition to cyber threats by introducing sublevels for probability as depicted in figure 4. This model requires understanding of the threat actors' intent, which requires a motivation and aims. Opportunity refers to the possibility for the actor to use its capabilities, for example, to exploit a vulnerability in a system. The fact that a system has a vulnerability does not make exploitation likely if there is no threat actor capable of exploiting it or willing to attack. Therefore, considering only vulnerabilities as sources of risk gives a biased picture of the total cyber risk.

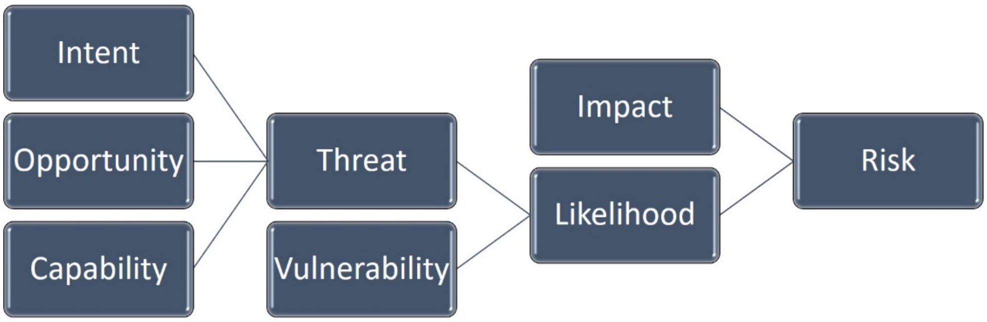


FIGURE 4 The role of cyber threats in risk evaluation (Bimco, 2020).

There is no consensus in the cybersecurity community regarding the terminology. For example, comprehensive ontologies for cyber-threat intelligence do not exist (Mavroeidis & Bromander, 2017). Moreover, "threat modeling" is an ambiguous term in this context (Xiong & Lagerström, 2019). A cyber threat is no easier to define than cybersecurity. Depending on the context, a cyber threat can refer to an adversary or to an attack by the adversary creating the threat (Bodeau, McCollum & Fox, 2018).

The definitions above are at a highly abstract level and are best suited for higher-level planning and strategies. The language used at lower abstract levels needs more detailed terminology. National strategies form the higher level, where technical details are at minimum. Another abstraction level is achieved while analyzing technical vulnerabilities or investigating a breach. Attack details at a high abstraction level are static, and in that description, a Denial-of-Service (DoS) attack only prevents a service from fulfilling it intended function. More detailed technical understanding of how the DoS was executed is required to prevent new types of DoS attacks. This is described at lower abstraction levels. The challenge is how to keep deeper descriptions updatable but still coherent enough to be sharable. An example of a high-level cyber-attack description is a cyber kill chain (CKC; Hutchins, Cloppert, & Amin, 2011), and a low abstraction level is achieved through indicators of compromise (IOCs) which directly describe the technical details demonstrated in an attack.

For this thesis, the Mitre ATT&CK (Strom et al., 2018) framework was chosen because it reflects the attack features seen in practical work and is updated when new forms of attacks are discovered. The framework presents medium-level abstraction between a CKC and specific vulnerabilities. The sources include threat intelligence reports, conference presentations, webinars, social media, blogs, open-source code repositories, and malware samples. Many security companies have adopted this framework in their reports. By using the framework in ePilotage, the same codes and names for attacks and methods will make it easier to compare own results with the results provided by the companies. ATT&CK comprises information on adversary groups and their software, techniques, and tactics. The ATT&CK model relationships are presented in figure 5. Moreover, ATT&CK has versions for mobile and industrial control systems, which broaden the framework's usability in complex environments (Strom et al., 2018; Alexander, Belisle, & Steele, 2020).

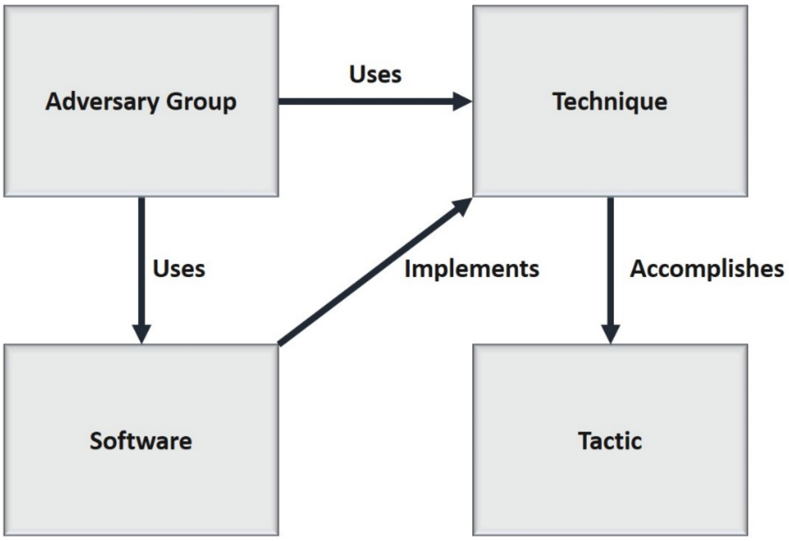


FIGURE 5 ATT&CK model relationships (Strom et al., 2018).

Although ATT&CK terminology can describe discovered adversary groups, the framework does not offer constructs for discussing group's attack motivation. For the motivational aspect, the sixfold classification model based on motivational factors (Lehto, 2020) is used to describe attacker archetypes. The model presents cyber vandalism, cybercrime, cyber sabotage, and cyber warfare as the basic constructs of the cyber-threat model. These factors are discussed in more detail in publication PVII.

2.7 Critical infrastructure

Rushby (1994) defined a critical system as "one whose malfunction could lead to unacceptable consequences." This definition is based on the possibility that the critical system is not functioning correctly, and this leads to a situation that has severe effects, severe enough to be intolerable. The definition does not address the cause of the malfunction.

Broadening the idea of criticality from the system to the infrastructure level presents CI. In Finland's Cybersecurity Strategy (Secretariat of the Security Committee, 2013), CI is defined to include "structures and functions indispensable for the vital functions of society." The definition includes physical facilities and electronic services. This means that if CI malfunctions, society faces severe difficulties. At the European Union level, maritime transportation and ports are identified as parts of ECI (The Council of the European Union, 2008).

Critical information infrastructure (CII) includes the infrastructure behind the information systems of the vital functions of the society (Secretariat of the Security Committee, 2013). Globally C(I)I is commonly seen as a subject of cyber threats (Luiijf, Besseling, & De Graaf, 2013), and protecting is forms a research branch of its own, Critical Infrastructure Protection (CIP).

2.7.1 Industrial control systems

Industrial control systems (ICSs) include a varied set of control systems used in the industrial setting in manufacturing or transporting matter or energy, many of which are included in critical infrastructure. ICSs includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLCs). The controls in the ICS settings can be automated or include human input through human–machine interfaces (HMIs). (Stouffer et al., 2015)

ICSs used to be isolated, but digitalization and device connectivity have brought cyber-attacks as a huge risk in the CI environment (Guo et al., 2020). As traditional ICT devices connect with these systems, the connectivity features transform toward current ICT solutions, including the internet and cloud computing (Bhamare et al., 2020). This progression entails modern cyber threats in new surroundings.

ICSs differ from ICT in many aspects that affect cybersecurity and the outcomes of cyber-attacks. One main feature is that ICSs often interact with the physical world directly through various actuators, valves, and breakers. These systems which combine features from computational and engineering disciplines are called CPSs (Baheti & Gill, 2011). An example of risks this feature introduces is compromising nuclear safety by affecting a nuclear power plant's ICS to cause reactors to shut down (Guo et al., 2020). Human safety arises as a key concept when major risks shift from delays in business operations seen in ICT to loss of life, equipment, or production in ICSs (Stouffer et al., 2015).

Other ICS-specific features include time criticality and high-availability requirements, varying geographic distributions (including vast distribution systems in, e.g., power grids), the presence of many proprietary operating systems and communication protocols, limited computing resources, slower software change processes, and extended component lifetime up to 15 years. Because of differences in ICT and ICS architectures, traditional cybersecurity solutions are not always suitable. In addition to industrial settings, ICS characteristics are seen in many other settings, such as transportation and logistics. ICS cybersecurity could be used as a reference to protect these systems (Stouffer et al., 2015).

2.7.2 Case Study: The cyber-threat landscape in the energy sector (PII)

RQ1: What type of cyber-attacks have occurred in critical infrastructure?

Energy production, transmission, and distribution include many features seen in ePilotage, such as critical infrastructure status, the presence of an ICS and a CPS, and the transformation from an isolated engineering environment to a connected smart setting. The benefit of examining cyber-attacks in the energy sector comes from the broader case material publicly available. The visibility on actual cyber-attacks in critical infrastructure including ICS elements contributes to this thesis. Although information about attacks against the remote pilotage environment is not available, the attacks described in PII provide current realistic capabilities, interests, and methods of cyber adversaries.

Highly targeted and non-targeted attacks are discovered. Targeted attacks focus on learning the targeted environment exactly. Non-targeted attacks are cases in which a generic widespread cyber-attack reaches an organization in the energy sector. This type of attack includes ransomware attacks. Often, this type of attack gains media attention quite rapidly, and the organization can prepare for it if the organization is not hit by the first wave.

Targeted attacks against energy companies vary from pure espionage to disruption of operations. The entry point does not have to be a unique ICS vulnerability but could be mundane spearphishing or an SQL injection attack. Once the foothold is established in the ICT network, the attack can achieve its goal there or advance to the ICS environment. The normal commands of ICS infrastructure are often adequate to cause disruptions. Additional challenges can be created by disrupting restoration operations or by clouding situational awareness. The acute situation may be solved quickly, but the full clean-up can take a very long time.

Status as a critical infrastructure operator means increased interest from the press to publish news of cyber events. Sometimes, the headlines are more provocative than accurate but require the target organization to comment on the situation. For ePilotage, this is especially likely if the cyber incident involves a risk of losing human lives or polluting the environment. Moreover, introducing new technologies could be difficult if there is considerable mistrust regarding the safety of the technology.

2.8 Systems and system thinking

2.8.1 System of systems

A system of systems (SoS) is composed of multiple independent constituent systems. An SoS can be described through eight dimensions: autonomy, independence, distribution, evolution, dynamic reconfiguration, emergence, interdependence, and interoperability. Autonomy refers to the constituent systems' rules and managerial independence. Independence refers to constituent systems' capability to function on its own. (Nielsen et al., 2015)

Discussing a complex system and the risks of hazardous events in physical reality recalls Perro's (2001) normal accidents. Normal accident theory claims that in systems where there are numerous complex interactions and close coupling without pauses, substitutions, diversions, or slack, there will inevitably be failures. This is due to multiple initial small failures cascading to a more dangerous outcome. One of the fields that Perro saw as likely to experience normal accidents was marine transportation. Although the events discussed in this thesis are not unintended accidents, the element of uncontrollability is present.

2.9 Maritime concepts and piloting in Finland

In pilotage, a pilot acts as an expert on local waters and their navigation, and as an advisor to the ship's master. In Finland, pilotage is mandatory in compulsory pilotage areas for vessels carrying certain hazardous cargo or longer more than 70 meters or have a maximum breadth of more than 14 meters. Exceptions exist in Saimaa Canal and for some separately defined vessels and situations. One exception is a Pilotage Exemption Certificate, which may be granted to a ship's master by the Finnish Transport and Communications Agency (Finlex, 2021).
Currently, many ships are equipped with digital safety and information systems, such as the Automatic Identification System (AIS) and the Electronic Chart Display and Information System (ECDIS). As some of these systems are mandatory, they are deployed in most ships today. For example, the AIS is mandatory for passenger ships and ships of over 300 gross tonnage (International Association of Marine Aids to Navigation and Lighthouse Authorities [IALA], 2004). It is likely that the systems will also form some part of future vessels'

systems, and thus, the vulnerabilities of today will be transferred to the future. Many of the systems are also dependent on generic technologies, such as GNSS for positioning and speed measurements or Very-High-Frequency (radio wave), VHF, for communication. Vulnerabilities in these technologies affect maritime traffic.

Originally, the AIS was developed to prevent ship collisions. According to resolution MSC.74(69), the AIS should be able to communicate with other ships to avoid collisions, with officials for identity and cargo information and with vessel traffic services (VTS) for traffic management purposes. The resolution also defines three types of data the AIS should provide: static, dynamic, and voyage related. Static data include the call sign, name, length, beam, type, and where the location of the position-fixing antenna on the ship. Dynamic data include the position, time, course, speed, heading, navigational status, and where available, the rate of turn, angle of heel, pitch, and roll. Voyage data include draught, cargo type, destination and estimated time of arrival, and an optional route plan. Moreover, the AIS may provide short safety-related messages. The information intervals vary depending on the information type and the ship's speed. Maritime Mobile Service Identity (MMSI) is used for identification. (The Maritime Safety Committee, 1998)

Resolution MSC.308(88), adopted in 2010, states that the AIS is subject to annual testing to verify the ship's static information, correct data exchange with sensors, and radio performance (The Maritime Safety Committee, 2010). Current AIS information is largely obtainable online through websites (MarineTraffic, 2021; Vesselfinder, 2021). For positioning, the AIS typically uses GNSS, but it may have a backup for GNSS failures (Bhatti & Humphreys 2017). The system also has VHF communication and thus, is susceptible to vulnerabilities of that technology (Tam & Jones, 2019a).

Moreover, the AIS is used outside vessels to enhance the operations of aids to navigation (AtoNs) devices and systems. These are called AIS AtoNs, and their AIS messages can come from the physical AtoN, delivered through a remote station, or exist only in digital reality without any physical device present (IALA, 2007).

ECDIS is the modern enhanced version of nautical paper charts. It combines electronic charts with the ship's position information using a multitude of sensors. Position information preferably should be confirmed by two separate sources. ECDIS should enable route planning, monitoring, and alerts if a ship is moving to unsafe locations (MSC.232(82)). Most ECDISs use the AIS and automatic radar plotting aid (ARPA) information and present it as an overlay. Discrepancies in information can be used to detect malfunctions and spoofing but require a trained crew (Bhatti & Humpreys, 2017). ECDIS is also a GNSS-dependent system (Son et al., 2020).

Ships have a voyage data recorder (VDR) onboard. It has a similar function as airplanes' black boxes: to store events during a voyage for future investigative needs. The records include date, time, position, speed, heading, bridge audio, communication audio, radar, AIS, depth, main alarms, and wind speed and direction (Tam & Jones, 2019a).

VTS is responsible for maintaining a real-time picture of the traffic situation. Ships 24 meters and longer are obligated to use the service. VTS provides information on matters related on safe marine traffic and navigation assistance. This requires reports when ships are entering the VTS area, before anchoring, before leaving an anchorage, after berthing, before leaving port, and at defined reporting points. Reports should include the name of the vessel, reporting point, destination, and intended route. VHF is used for communication between a ship and VTS. In exceptional situations, VTS can restrict the use of a fairway. (Fintraffic, 2021)

The Pilotage Act regulates pilotage in Finland, and Finnpilot is responsible for arranging pilotage of vessels in Finnish waters. A ship's pilotage begins by ordering a pilot through digital channels via an app or email. This can be done well in advance. There are designated pilot boarding places where the pilot boards or disembarks vessels. Amendments to the Pilotage Act made in 2019 also set requirements for remote pilotage. A permit is issued for a fixed time period of no more than five years. Renewal is possible after the period. It is required that the remote pilotage does not put vessel traffic at risk, harm the environment, or impede vessel traffic. The remote pilotage permit determines where remote pilotage is allowed and the ships participating in it. The permit also may have restrictions related to weather and ice conditions. The ship's master has the right to refuse remote pilotage, and this must not affect the availability of pilotage. (Finlex, 2021)

Autonomous ferries and ships have been tested in different projects. The estimations of when full operational capability is achieved vary. Kooij, Colling, and Benson (2019) constructed a technological forecast and concluded that technological barriers do not hinder full-scale adaptation, but economic viability is a challenge. Currently, the manned option is cheaper, but as technology matures, this situation will change. The estimation of the time ranges for this varied greatly, from 2026 to 2041 for data transfer, from 2037 to 2101 for cargo handling, and from 2025 to 2060 for fuel cells. The authors acknowledged that they did not estimate all challenges for autonomous shipping. One concern they raised is intentional disruption, for example, by hacking data signals.

In 2018, Rolls-Royce and FinFerries together presented the autonomous ferry *Falco* and demonstrated its capabilities to navigate and berth without human control (Rolls-Royce, 2018). This journey was supervised from a shore station.

Yara Birkeland was advertised as the first electric zero-emission, autonomous container ship. The project is a partnership between fertilizer company Yara and technology company Kongsberg and started in 2017. The Covid-19 pandemic caused delays, but the vessel was delivered in November 2020. However, it is not yet operational due to challenges in autonomous logistics on land. Yara is aiming to complete the project in the future. (Yara, 2020)

In 2020, *Mayflower Autonomous Ship* was launched, and it is expected to cross the Atlantic in 2021. It is an autonomous research vessel from ProMare and IBM designed to gather data from the ocean. (Levin, 2020)

One step closer to a functional ecosystem is the launching of Massterly, a company set up to offer services for the entire value chain for autonomous ships. They state that currently fully autonomous and unmanned vessels are better suited for short and predictable routes, but they aim to expand to deep sea shipping (Massterly, 2021). An example of the business is a signed contract to deliver in 2022 two autonomous vessels to transport cargo across Oslo fjord. (Kongsberg, 2020)

2.10 Previous and related research

Previous and related research for this thesis covers multiple topics. Cybersecurity of maritime transportation is naturally the closest relevant research topic. Most of this research discusses the cybersecurity of a ship at different levels, focusing on either a single technology or the whole autonomous ship. Autonomous ship research consists of more than just cybersecurity. The safety aspects have been examined intensively.

As research on cybersecurity in maritime transportation is limited, other sources are used. As near-field research, CI cybersecurity offers a much broader collection of publications. ICS and CPS cybersecurity issues are presented in this field.

The widest set of publications is offered by general cybersecurity research. The challenge arises from selecting relevant topics. The most beneficial material is found from understanding the general trends and attack features of different types of adversaries. In addition, this field provides information on possible spread of general malware types that do not target a certain organization but have large numbers of collateral victims.

2.10.1 Maritime transportation cybersecurity

Ten years ago, the European Union Agency for Cybersecurity (ENISA; 2011) published the results of a workshop discussing maritime cybersecurity. The situation in 2011 was not promising, as one of their main findings describe it:

> "The awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent."

This highlights that in the maritime field considering cybersecurity is a new phenomenon. In 2011, there were issues regarding awareness that cybersecurity was even an issue, the complexity of the technological environment, fragmented governance, the lack of regulation, and the absence of a holistic view of maritime cyber risks. Although there has been advancement, recent reports state that understanding and using cybersecurity practices are not yet fully utilized in the maritime sector (Alcaide & Llave, 2020).

Since 2011, the maritime industry has published guides and recommendations for cybersecurity in the maritime environment.

In 2017, the International Maritime Organization (IMO) published guidelines for managing maritime cyber risk (IMO, 2017). They include high-level recommendations on cyber risk management. The increase in digitalization and networked environments created the need for this type of resolution. The presence of operational technology environments on top of ICT environments is noted, but the focus is not technical. The resolution proposes cyber-risk management starting at the senior management level and including the functional elements identify, protect, detect, respond, and recover.

The Maritime Safety Committee published resolution MSC.428(98) in 2017, which affirms that safety management systems should consider cyber-risk management (The Maritime Safety Committee, 2017). The resolution refers to the IMO's guidelines for managing maritime cyber risk. The resolution states that cyber risks should be addressed in safety management systems before the first annual verification of the company's Document of Compliance after January 1, 2021.

In 2019, ENISA published a report on port cybersecurity. The report presented the status of port environment cybersecurity, related policies, a high-level reference model of threats, attacks, and security measures, and a comprehensive asset taxonomy. Threats and attacks were used to create sample scenarios which were analyzed. The purpose of the publication is to serve as a reference point to promote collaboration and awareness of port cybersecurity in the European Union.

In 2020, Bimco published the fourth version of guidelines for cybersecurity onboard ships. The guidelines cover the basics of cybersecurity and risk assessments. In addition, they present case stories of cyber incidents. The stories are short and aimed to clarify certain aspects of security recommendations. The guidelines focus on ship and ship-owner systems, and the larger SoS in which the ship functions is mentioned occasionally. Key takeaways for ePilotage include the understanding that ships' cybersecurity preparedness levels seem to vary greatly, and the more data connections and smartness in the system, the more cybersecurity understanding is required. For example, the guidelines propose that there should be personnel on board who are able to understand and interpret IDS alerts. However, basic cybersecurity practices should be addressed first. For example, outsiders using USB drives have caused malware infections in air-gapped ship systems.

Technologies included in current ships have been examined in multiple publications. For ePilotage, these technologies are interesting, as they will be present in fairways due to the traffic of traditional ships. Moreover, these technologies likely will be included in automated ships as use is often mandated.

Balduzzi, Pasta, and Wilhoit (2014) conducted a security evaluation of the AIS and experimentally confirmed their results with a novel software-based AIS transmitter. Their attacks were categorized as spoofing, hijacking, and availability disruption. They also considered whether an attack comes via software, radio frequency, or both. Identified attack scenarios include ship spoofing, aids-to-navigation spoofing, collision spoofing, search-and-rescue-transponder spoofing, false weather forecasting, AIS hijacking, and availability disruption through slot starvation, frequency hopping, and timing attacks. Based on the software evaluation, the authors stated that all three online AIS providers were susceptible to attacks. The challenges arose from the lack of confirmation of the source of the AIS information and the validity of the information itself. The researchers were able to create nonexistent ships and report low tide at a closed lake. They also were able to intercept and modify a valid AIS message with their own AIS gateway. On the radio frequency side, they were able to spoof vessels and buoys, hijack the AIS by overriding legitimate traffic with a stronger signal, and deny availability with multiple methods. The availability attacks consisted of using control messages that had higher priority than normal AIS traffic thus overriding them. Control messages were also used to instruct other AIS senders in the area to change their transmission intervals either to too long, to deny transmission, or to too short, overflooding the legitimate AIS receiver. A slot starvation attack reserved all AIS address space preventing all nearby stations from operating. Frequency hopping was used to fake an authority ordering AIS users to use frequencies not in use. The radio frequency attacks were tested to function from at least from 8.00 and 16.5 km distance with output powers of two standard AIS transponders (class B and class A). Most of the presented attacks included impersonating an entity, either a vessel, buyo, or an authority. The challenge of verifying the origin of the message presents a very real threat to maritime safety.

In 2016, Jones, Tam, and Papadaki (2016) presented cyber-attack scenarios for modern, but not automated, ships. These scenarios include malicious cargo that affected maritime communication once onboard, stealing cargo with the help of information obtained from the cyber environment, altering digital charts causing a shipwreck, controlling propulsion systems to hold passengers as hostages, controlling a ship to use it to collide and destroy other structures, and exploiting vulnerabilities by using drones while the ship is at sea and unable to patch. The authors saw that a human crew is an advantage in maintaining security as they are able to verify systems' status. This requires training for the crew to understand the cyber-attack possibility.

Bhatti and Humphreys (2017) discussed controlling ships via false Global Positioning System (GPS) signals. The authors presented alternative methods for cross-checking GNSS information but stated that they could not detect a subtle attack masquerading as ocean current before the deviation became hazardous. Cross-checking with AIS results was stated to be bad for two reasons: The AIS is easily spoofed and depends on GNSS. The ARPA functioned in collision avoidance with radar-reflective objects because it does not depend on GNSS but will not detect underwater hazards. The results were demonstrated onboard a vessel in open waters. Position deviations are even more dangerous in limited conditions such as in a fairway, and the tolerance margin is much smaller. Therefore, position attacks are a threat to consider for ePilotage.

Medina et al. (2019) also discussed GNSS-related threats in the maritime context. A GNSS jamming experiment was presented. The influence area was discovered to be 3 km wide at parts. Countermeasures were divided into three categories: alternative terrestrial radio navigation system, GNSS receiver's internal signal processing techniques and adaptive antenna arrays, and a multi-sensor fusion scheme with independent onboard sensors. The strength of the satellite signal in the jamming test functioned reasonably well to detect jamming.

Son et al. (2020) tested the positioning capabilities of eLoran. They hoped it would be a useful alternative for GNSS during a jamming attack. The authors also hoped that accuracy of 20 m they achieved could be decreased to 10 m after further research. This would fulfill the IMO's regulation of accuracy for maritime navigation systems (Son et al., 2020).

Svilicic et al. (2019) tested a recently installed ECDIS with a vulnerability scanner, Nessus Professional. They were able to identify nine risky vulnerabilities and information on the ECDIS's underlaying services. The most critical vulnerabilities related to an obsolete version of the Apache web server. Medium risks related to Server Message Block (SMB) version 1, use of which is not recommended due to the lack of security features. Moreover, the ECDIS was running on an operating system (Windows 7 Professional service pack 1) whose support was ending later that year. The web server and SMB were not mandatory for regulated functionality of the ECDIS software. For ePilotage, this describes the complexity of ensuring the security of all involved systems. If there are extra features in systems that present vulnerabilities, how can they be evaluated and tested? A vulnerability scan found them in one separate system while the ship was docked, but organizing this more broadly is difficult.

Tam and Jones (2019a) presented a model-based framework for Maritime Cyber-Risk Assessment (MaCRA). The framework evaluates a ship's cyber-risks based on vulnerabilities, ease of exploit, and gained reward. They presented vulnerability estimations for multiple current onboard technologies, such as ECDIS, AIS, and GNSS. They stated many of these technologies depend on other technologies. For example, the ECDIS depends on the AIS, and the AIS depends on GNSS. They saw low interest for attackers in Navtex, sonar, and anemometers. Insiders have access opportunities, for example, to VDR, which could enable destruction of evidence of an event. eAtoNs might attract attackers because it is not always possible to confirm the data with physical observation. The authors stated that although they presented a large set of vulnerabilities in their paper, a complete list of maritime systems and their vulnerabilities does not exist.

One set of studies focused on surveying the status of maritime cybersecurity in the field with questionnaires. Although the situation has improved from 2011, more training is wanted.

Tam and Jones (2019b) conducted a survey to explore maritime cyber-risk with 75 participants, who mainly consisted of mariners and port officials (65 %); 14 % were trainers/trainees. The remaining participants were higher management and high-ranking security specialists. Regarding standards, crew training was seen as the most concerning problem in the maritime industry, but the second concern was cybercrime and cyber-attacks (55.2 % of the respondents); 60.7 % had not had any training in cybersecurity but saw cybersecurity training as beneficial. Actions right after a cyber-attack varied. Most (67.3%) would engage backup systems, or anchor the vessel (30.9 %), or continue to port (23.6 %). 24.6 % would rely on re-booting the systems. After the initial response to the attack, a high majority (85.7 %) would rely on shore-based experts to examine vessels security status. However, 16.1 % would just give generic advice to wipe and re-start systems.

Alcaide and Llave (2020) investigated knowledge of cybersecurity of maritime professionals (individuals working in terminals, ports, ships, and other sectors) through an online questionnaire. The results showed some concerning negligence of cybersecurity's best practices. For example, 40 % of the respondents stated that they shared passwords with others. In addition, working on personal devices was very common. The respondents saw cybersecurity solutions as mostly technical implementations. However, the researchers saw a demand for training due to the lack of knowledge. In addition to training, cyber resiliency agendas were seen as important because they would aid in solving a crisis caused by a cyber-attack.

The publications above described the current situation. There are studies concerning future maritime solutions, such as autonomous ships and fairways.

Ahvenjärvi (2016) discussed how the human element will change with autonomous ships. Although decisions seem to be shifting away from humans, this is only partially true, as humans are behind the design and creation of automated behavior. Software errors and decision algorithms will raise the question of responsibility when something unexpected and unwanted happens. Moreover, Ahvenjärvi noted that humans will easily start to trust automation too much and neglect safety procedures and manual checks. As a disclosure, the author noted that although automation would decrease the effect of some types of human errors, the adaptation to surprising situations would be weaker. This requires attention to the resiliency of autonomous ships and their control systems to ensure safety.

Kavallieratos, Katsikas, and Gkioulos (2018) identified a ship's cyber systems and proposed a system architecture for a cyber-enabled ship (C-ES). They also conducted a cyber-attack risk evaluation using STRIDE. The C-ES architecture includes systems, such as AIS, ECDIS and GMDSS, already used in traditional ship, and the authors concluded that these systems have especially high risks. Upward risk propagation in systems was seen as resulting in high overall risk for the bridge automation system and the shore control center. Lower risk levels were associated with engine automation systems.

In 2020, Bolbot et al. employed cyber preliminary hazard analysis in a case study to assess cyber risks of inland autonomous ships. The waterway differs from open sea in a shorter distance to shore which enables physical attacks, for example, by terrorists. From the safety aspect, the most dangerous attacks target shore control stations and ship control stations. In addition, malware installation on the collision avoidance system and the situation awareness system has high safety implications. Recommendations included adding firewalls between different control zones, deploying intrusion detection systems, and eliminating internet communication links.

Lahtinen et al. (2020) examined the risks of remote pilotage in an intelligent fairway. Their approach was safety centric, and they did not discuss cybersecurity challenges. A survey of the accident statistics of Port of Rauma showed that currently a pilot on board does not remove human error. To decrease the possibility of human error, better situational awareness is needed. This requires strong communication between the vessel crew, pilot, and VTS. For remote piloting and intelligent fairways, the authors stated that technology could increase efficiency and safety by creating more holistic situation awareness. However, this does not eliminate human error, and the risk is barely transferred to the shore station. In addition, in remote operation audible, visual, physical, and behavior-based information is lost and must be compensated with novel data. The more complex environment also requires additions to the Safety Management System (SMS) to encompass the structural requirements arising from social and physical environment effects. The need for strong communication between participants remains.

The maritime industry is moving toward awareness of cybersecurity, and training is seen as beneficial. However, from the technical perspective many ship systems have vulnerabilities, and updating them may be more uncontrolled than in traditional ICT systems. For the automated future, many of these vulnerable systems will be present, either in traditional vessels among automated vessels or as parts of automated vessel systems. Moreover, the possibility for human error is not removed but the risk may transfer to a different location in the chain of events. Therefore, the risk evaluations should be updated, and new risk scenarios developed.

2.10.2 Critical infrastructure, ICS and CPS cybersecurity

Publications on cybersecurity outside the maritime context offer case studies as seen in publication PII. Other beneficial material comes from models, methods, and recommendations. Specifically, CI, ICS, and CPS cybersecurity publications offer valid information for ePilotage.

International CI is addressed in multiple programs and frameworks. The general focus is to raise awareness and to incorporate cybersecurity aspects in organizations' processes. In addition, CI security issues outside cybersecurity may be examined. For example, in the European Union, the European Programme for Critical Infrastructure Protection (EPCIP) focuses on terrorism, although this program can also address all other relevant threats (European Commission, 2006). In 2018, the National Institute of Standards and Technology (NIST, 2018) published a framework for improving the cybersecurity of critical infrastructure. The objective is to include cybersecurity aspects into organizations' risk management processes. These frameworks and programs are at the high abstraction level.

On the practical side, recommendations for ICS security have many of the same elements as traditional ICT security: segmentation, firewalls, an IDS, and two-factor authentication. The difference comes from the vulnerability of the ICS environment as the life-cycle is much longer, and the design process is not security centric. Therefore, a defense in depth approach is recommended, and for example, direct outside connections to the ICS environment should not be allowed. (Obregon, 2015)

The other difference compared to traditional ICS security is that the attacks in cybersecurity are different due to the larger geographic distribution of assets. An ICT environment may reside in an office building, and CI may have ICS components residing far away from central locations. Thus, they are more susceptible to physical attacks. Physical security should not be considered separately from cybersecurity, as attacks may involve attacking through cyber access against physical assets (opening electronic locks remotely) or through physical access against cyber assets (breaking in and having access to control system elements; Depoy et al., 2005).

The impacts of a major ICS attack have often caused consequences in the physical reality. Production shutdowns and delays, safety system violations, and power outages make cyber-attacks more concrete. Moreover, conventional attacks, such as data thefts and ransomware, are not excluded from ICS organizations (Alladi, Chamola, & Zeadally, 2020).

Cyber-threat aspects specific to CI for financial institutions have been examined. The role of financial institutions in modern society is critical, as many services require these institutions to function. Bodeau, McCollum, and Fox (2018) surveyed cyber-threat modeling frameworks. Because none of the surveyed frameworks were sufficient to meet the authors' needs, they developed a threat modeling framework for medium-to-large organizations in critical infrastructure sectors, especially aimed at financial services. The authors presented a high-level framework with initial assigned values for some of the key constructs. The authors wanted to ensure concise consideration of cyber threats among different stakeholders. For adversarial threats, the key constructs are intent, targeting, and capabilities. The sub-characteristics of intent, goal, or motivation include financial gain, personal motives, geopolitical advantage, and positional/stepping stone which meant acquiring something to be used in further actions. Targeting describes the scale of the effects and the targeted assets. Capabilities form categories based on available resources, methods, and attack vectors. The authors assigned different adversary goals to the typical actors, but they are not individually characterized or described. Very high-level threat scenarios for the financial sector are presented as the starting point for more detailed scenarios. These scenarios were adapted from previous work (Bodeau & Graubart, 2017) and included only a few sentences per scenario.

Bodeau and McCollum (2018) extended their previous work (Bodeau, McCollum, & Fox, 2018) on threat modeling to the financial services sector by considering the SoS aspect of the threat model. Challenges arising from this aspect were seen in unified risk governance, visibility due to lack of sharing, use of the appropriate level of abstraction in scenarios, complexity in systems and their dependencies, and external dependencies, for example, in supply chains. Threat model constructs presented in a previous publication (Bodeau, McCollum, & Fox, 2018) remained, but Bodeau and McCollum tailored the targeting by considering three scopes: technical, functional, and institutional. The technical scope addresses whether the adversary targets a specific technology within the SoS, for example, a single operating system or multiple environments. The functional scope addresses whether the adversary targets a certain function of the SoS and the institutions involved in it or whether the adversary attacks a broader function, such as the domain name system. The institutional scope addresses whether the adversary targets a specific institution or similar institutions. In the first case, the adversary may collect precise information on the institution, whereas in the latter case, the adversary focuses on finding something the institutions have in common, such as a widely used vulnerable application. New characteristics are also added to targeting. These address the adversary's control strategy for propagating the attack and how tightly it is directed, and institutional targeting which discusses attacks against the weakest link in the SoS. For SoS scenarios, a set of SoS characteristics is needed. They include the structure, defense capabilities, and decision model. A SoS scenario may include multiple adversaries that have different relationships. A SoS threat scenario in the financial sector was presented as an example. This scenario was detailed and included descriptions of the target, adversary profiles, actions, and timing. The scenario described the effects of multiple malware infections by two criminal groups.

Fox et al. (2018) expanded Bodeau's threat model (Bodeau, McCollum, & Fox, 2018) with ATT&CK and Capec information to describe attacks against the financial sector. The authors saw existing attack repositories forming a strong foundation for detailed information but stated they lacked information on some environments, such as clouds and hypervisor infrastructures. As a final note, Fox et al. addressed the need for continuous updating of models as adversaries change their behavior and methods.

2.10.3 Cybersecurity trends and events

The cybersecurity scene changes rapidly, and academic publications are not always able to respond to the latest events. Therefore, it is essential to consider non-academic source material especially in future system design and building. Then, following cybersecurity trends and events will ensure the system is built for a realistic environment. One source for this information are white papers published by cybersecurity companies. These materials include trend reports which describe cybersecurity events at a highly abstract level and attack descriptions that may have detailed technical analysis of recently discovered cyber-attacks.

Ponemon Institute (2018) surveyed more than 1000 senior information technology practitioners to find out the future megatrends in cybersecurity. Their findings revealed that the insecure Internet of Things (IoT) was seen as one of the key threats. In addition, ransomware was seen to be more frequent in the future. Although data breaches for large volumes of data were seen posing the highest current risk, breaches involving high-value information were the greatest risk in the future. Moreover, breaches that damage critical infrastructure were considered a future risk. The risk that increased the most was cyber warfare or cyber terrorism, but nation-state attackers were still seen to pose higher total risk in the future. For organizational risks, the integration of third parties into internal networks and applications was the most concerning future issue followed by lack of qualified information technology security personnel.

Fireeye Mandiant Service publishes the special report *M-Trend* on observations and predictions on cybersecurity issues annually. The report includes statistics and ATT&CK-based descriptions of the most common attack methods and features contemporary phenomena. The 2021 report (Fireeye, 2021) examined events from October 1, 2019, to September 30, 2020. The report states that globally organizations have improved their own detection capabilities, and attacks are discovered faster than before. The shorter dwell time is partly a consequence of increased ransomware cases where detection is fast due to the attack type. However, in the Europe, Middle East, and Africa (EMEA) area, dwell times increased from 54 days in 2019 to 66 days in 2020. In the EMEA, 28 % of attacks were discovered within one week or less, but 8 % had dwell times longer than three years. Although ransomware is increasing, it is also evolving from simple demand of payment to decrypt files to multifaceted extortion. In addition to encrypting files, this new type includes theft of sensitive data, publication of stolen data, and additional coercive tactics, including contacting the media, employees, and the target organization's business partners. Moreover, DoS attacks are used to further disrupt operations during ransomware attack. Having file backups is no longer a comprehensive recovery strategy against ransomware. The report presented several steps for mitigating the risk of ransomware attacks. These steps include hardening the systems, especially highly privileged accounts. For recovery, the report stated that information obtained from the attack before starting restoration is crucial. This includes facts from log entries, which empower the restoration with information about where the attacker has infiltrated, how the attack is controlled, and whether it is possible to stop and contain the ransomware.

In the Fireeye (2021) report, ATT&CK was used to communicate general attack statistics, such as frequently targeted technologies (T1021.001 Remote Desktop Protocol, T1569.002 Windows Services, T1059.001 PowerShell), initial access methods (T1190 Exploit Public-Facing Applications, T1566 Phishing, T1133 External Remote Services, T1078 Valid Accounts), and impacts (T1489 Service Stop, T1529 System Shutdown/Reboot, T1490 Inhibit System Recovery, T1486 Data Encrypted for Impact). The most frequent initial accesses come from either vulnerable outside interfaces or human behavior enabling the access. The use of valid accounts has been observed in trend reports, but it has also been used in CI attacks against Ukraine's energy sector described in PII. Lateral movement through remote services such as remote desktop protocol, SMB/Windows admin shares, SSH, and Windows remote management function in a networked environment but also replication through removable media is being used. This provides an overview of the generic approach a cyber-attacker takes. The use of ATT&CK codes and names make comparison to other data sources using ATT&CK possible. Moreover, following trends is easier with unified expressions used through the followed time period.

2.11 Conclusions

This thesis investigates a phenomenon that has aspects in many different and often separate fields of research. Therefore, an exploratory approach through a case study was chosen to illuminate various sides of the challenge. As a result, a cyber-threat model and scenarios are presented, but the thesis points out the direction rather than including all the details. In the everchanging cyber environment, it would be hazardous to claim a challenge has been solved permanently.

Related literature consists of many publications on high-level maritime cybersecurity, ship cybersecurity, and technological vulnerabilities. Studies have been conducted on the cybersecurity of autonomous ships, but for the entire smart fairway setting, cybersecurity is not extensively discussed. This thesis greatly benefits from previous research and in addition, provides a view of cybersecurity applied to the remote piloting environment.

The cyber field is changing, and attacks are evolving to more complex entireties. Keeping up with the changes involves noticing trends in attacks, targets, and attackers. Unified framework with stable and clear expressions, such as ATT&CK, enables tracking long-term changes and enables knowledge sharing. ePilotage includes a large number of connections due to the high number of stakeholders. In this type of environment being able to share information precisely is valuable.

The cyber trends confirm that concern for cybersecurity of fairway navigation as part of critical infrastructure is a very important issue in modern society. The concern is not lessened by known vulnerabilities found in technological environments and the absence of cybersecurity awareness in the maritime sector. The cybersecurity of larger SoS structures in smart fairways has not been examined extensively. Therefore, this thesis provides a unique understanding of the aspects related to cybersecurity of remote pilotage.

Cyber-threat trends are often directed at traditional ICT environments, but as ePilotage is also a target of these trends, the key takeaways are beneficial. According to the Ponemon Institute report, awareness of CI cyber risk is present. In particular, the report stated that the desired impact could be to cause damage. For ePilotage, this means that considering the worst-case scenarios of intentional shipwrecks is relevant and should not be ignored. The importance of ransomware and changes in data breach behavior were present in the Ponemon Institute and Fireeye reports. Data breaches that are more targeted mean for ePilotage that not only large-volume data storage should be considered a target. Thorough consideration and understanding of the value and importance of the protected data are needed.

ePilotage faces a complex and evolving cyber-threat environment. One source for updated information that is relevant for ePilotage does not exist; the picture of the situation is created from multiple sources that must be followed, combined, and filtered. This basic knowledge base of cyber threats is used in the next chapter and combined with unique features of ePilotage to estimate possible attack paths and consequences.

3 CYBER SECURITY IN THE EPILOTAGE SYSTEM

3.1 Introduction

Approaching a port in a fairway through an archipelago or in otherwise challenging circumstances differs from maneuvering at open sea where the margin of tolerable error is wider. Most accidents in fairways are caused by human error, and increased automation is seen as a solution to enhance safety (Lahtinen et al., 2020). Cybersecurity is becoming a major concern in shipping due to connected and integrated ICT networks, and cyber risks have been estimated only to increase in the future (United Nations Conference on Trade and Development [UNCTAD], 2020).

Maritime transportation and the operation of ports are essential to society's functioning due to the large percentage of cargo transportation. In 2019, 84.4 % of all of Finland's foreign trade goods (export and import) were transported by sea (Tulli, 2020). Tulli's (2020) statistics show that for some products sea transportation dominates. For example, 97.4 % of imported mineral oil and products are transported by sea. In addition to the economic impact, a disruption would affect society's functions that are dependent on imported goods. For example, transportation by roads is dependent on the fuel reserves. The magnitude of the effect would depend on the duration of the disruption and society's preparedness. This dependency categorizes maritime transportation as critical infrastructure for Finland.

Ships and ports have machines that interact with our physical surroundings. These machines include ship engines and cranes at ports. They form the CPS aspect of ePilotage and often include ICS components. Increased automation requires linking these systems to ICT systems for enhanced operations and surveillance. This introduces risks arriving to ICS environment through the ICT network as the number of access points increases. In ICT systems, cybersecurity is often understood as an important aspect, but is the cybersecurity of CPSs understood by their operator? Do ICT cybersecurity specialists understand the functioning of the CPS environment well enough to secure it? The communication between the personnel responsible for these environments needs to be close, and the transition point from one network to other carefully thought out.

3.2 Objective and organization of the chapter

The objective of this chapter is to present a description of the ePilotage SoS and related cybersecurity aspects through the thesis publications PIV-PVII. PI and PIII present discussion on intrusion detection methods that could be utilized in ePilotage environment. Furthermore, PIII provides insight of attack behavior observed from honeypot experiment. Chapter provides answers to research questions 2 – 9.

3.3 ePilotage

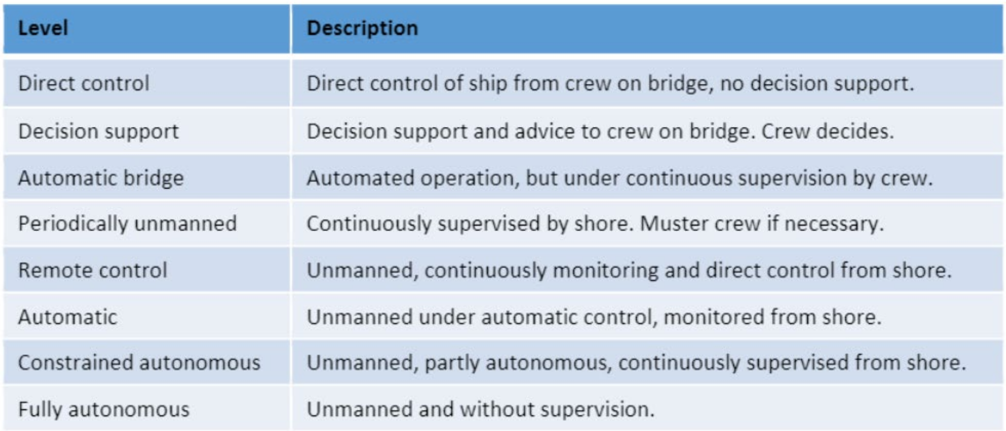
3.3.1 Basic elements of cybersecurity for an automated remote pilotage fairway system (PIV)

RQ4: What does the ePilotage environment consist of? (PIV)
RQ5: What are the cybersecurity elements of ePilotage? (PIV)

Publication PIV describes the background and environment in which ePilotage is designed to function and presents its basic constructs related to cybersecurity. The main results of PIV are the components affecting cybersecurity of ePilotage arranged according to the Maritime Security Management System (presented in figure 8) and the description of ePilotage functions, which are presented in a block diagram in figure 9.

Increased automation will require changes in current pilotage. Ultimately, when an automated ship arrives at the pilotage area, no human operators will be on board. This will require digital fairway and ship information as a substitute for traditional observations. This transformation to more dependency on digital information is one of the main differences between ePilotage and traditional pilotage. Before full automation, there will be different levels of remote operations. Therefore, remote pilotage is also an option onboard traditional vessels that may still have human crews.

During the transformation period, a mixed set of ships will arrive at ports. The average ship in the merchant fleet is more than 20 years old (Statista Research Department, 2020). It is not possible to change all ships to automated ones very quickly. Until then, different autonomy levels in maritime traffic will occur. One categorization of these levels according to Rødseth and Nordahl (2017) is listed in figure 6. The steps toward fully autonomous ships progress through the decreased presence of humans onboard and in control. First, the human element is transferred to shore to control and supervise the actions, but ultimately, ship functions will be unmanned and unsupervised.



Level	Description
Direct control	Direct control of ship from crew on bridge, no decision support.
Decision support	Decision support and advice to crew on bridge. Crew decides.
Automatic bridge	Automated operation, but under continuous supervision by crew.
Periodically unmanned	Continuously supervised by shore. Muster crew if necessary.
Remote control	Unmanned, continuously monitoring and direct control from shore.
Automatic	Unmanned under automatic control, monitored from shore.
Constrained autonomous	Unmanned, partly autonomous, continuously supervised from shore.
Fully autonomous	Unmanned and without supervision.

FIGURE 6 Autonomy levels for ships (Rødseth & Nordahl, 2017).

Similarly, as ships progress toward full autonomy, pilotage needs to adapt. Digitalization first introduces aids for ship crew and pilots and progresses toward moving pilots onshore. Perhaps in the future, pilotage can also be fully autonomous, but it would require massive development through the previous steps. The DIMECC's vision of the ePilotage environment is depicted in figure 7. The figure shows how additional sensor networks enhance fairways where ePilotage is located onshore.

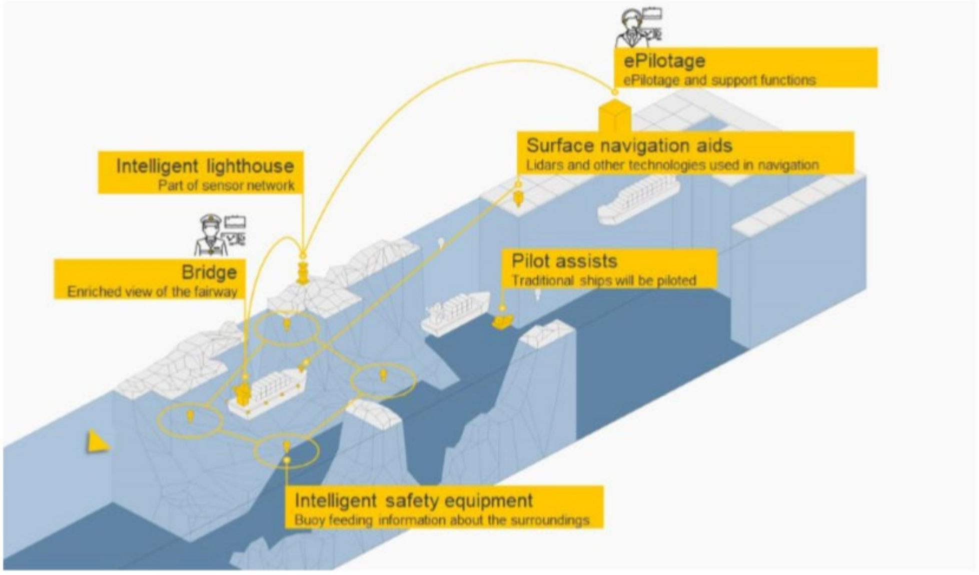

ePilotage
ePilotage and support functions
Intelligent lighthouse
Part of sensor network
Surface navigation aids
Lidars and other technologies used in navigation
Bridge
Enriched view of the fairway
Pilot assists
Traditional ships will be piloted
Intelligent safety equipment
Buoy feeding information about the surroundings

FIGURE 7 The ePilotage environment of the future (DIMECC, 2020).

As ePilotage is a large undertaking involving many organizations, stakeholders, and systems, it is important to identify them. The Maritime Security Management System (MSMS; Thai & Grewal, 2007) was used as a framework to map ePilotage's cybersecurity features. This framework emphasizes different aspects of ePilotage and is depicted in figure 8. ePilotage is designed to produce remote pilotage where stakeholders include different operators, services, and authorities. Their organizational relationships include their mutual relationships but also each stakeholder's relationships with their own cybersecurity providers, and other intra-organizational or other stakeholder relationships. Security dimensions include systems, which are discussed later in this chapter, as well as process continuity, security awareness, education, and training. Security elements can be divided into people, processes, and technology. Finally, the criteria present different abstraction level views that must be considered. This paints a picture of a highly interconnected network of actors, assets, and relationships that need to function together to secure the whole.

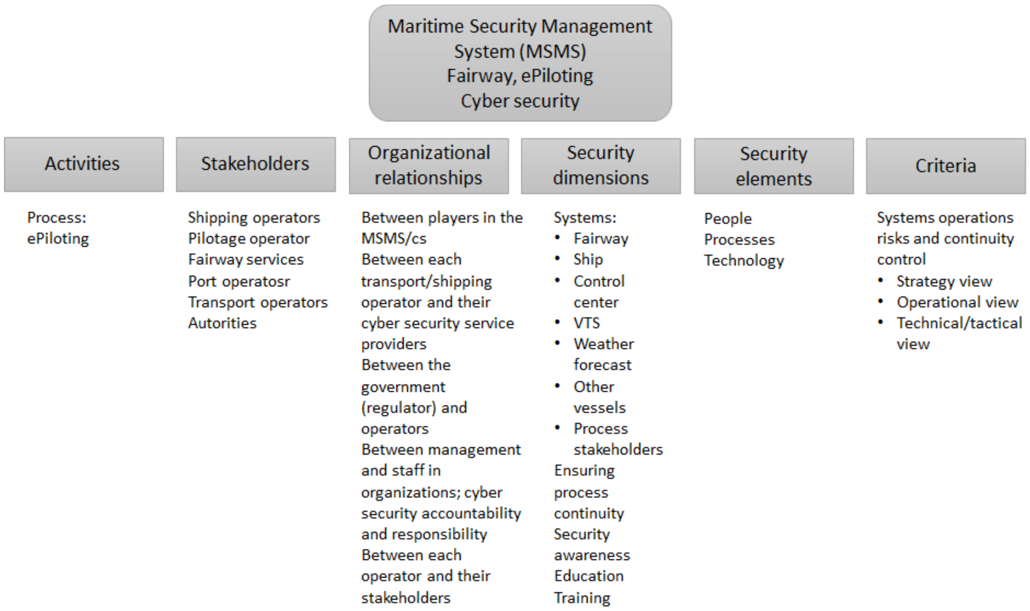

Maritime Security Management System (MSMS) Fairway, ePiloting Cyber security
Activities
Stakeholders
Organizational relationships
Security dimensions
Security elements
Criteria
Process: ePiloting
Shipping operators
Pilotage operator
Fairway services
Port operatosr
Transport operators
Autorities
Between players in the MSMS/cs
Between each transport/shipping operator and their cyber security service providers
Between the government (regulator) and operators
Between management and staff in organizations; cyber security accountability and responsibility
Between each operator and their stakeholders
Systems:
• Fairway
• Ship
• Control center
• VTS
• Weather forecast
• Other vessels
• Process stakeholders
Ensuring process continuity
Security awareness
Education
Training
People
Processes
Technology
Systems operations risks and continuity control
• Strategy view
• Operational view
• Technical/tactical view

FIGURE 8 ePilotage presented via the Maritime Security Management System framework (publication PIV).

The key systems in ePilotage are fairway systems, ship systems, and the control center. These systems are presented in the middle row of figure 9. The support systems include other vessels, VTS, weather forecast operators, and stakeholders' operators. These support systems are depicted in the top and bottom rows of figure 9. Together, these systems form the key set of functionalities and are used in publications PV and PVII to act as the framework presenting ePilotage. Fairway systems include a set of sensors and smart objects, such as intelligent lighthouses or buoys. Ship systems include their sensors, information systems, and controls. The automation level varies depending on the autonomy level of the vessel.

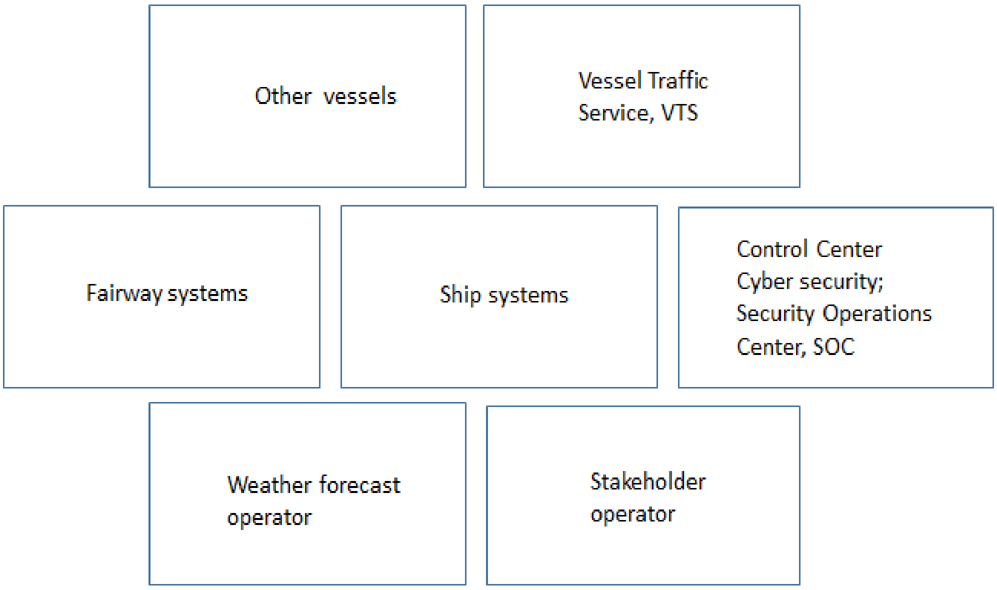

Other vessels
Vessel Traffic Service, VTS
Fairway systems
Ship systems
Control Center Cyber security; Security Operations Center, SOC
Weather forecast operator
Stakeholder operator

FIGURE 9 ePilotage functionalities in a block diagram (publication PIV).

In conclusion, ePilotage includes many different views of on cybersecurity and many interconnected systems and actors which have their own dependencies outside ePilotage. This creates challenges in communication and situation awareness to secure the whole system.

3.4 Intrusion detection systems

Intrusion detection systems (IDSs) are designed to detect malicious traffic either by comparing the traffic to known signatures or by detecting anomalies. Signature-based systems can detect known malicious activities but may miss new versions. Anomaly detection can react to new types of attacks but may produce false alarms more often. IDSs can be deployed in the network as a network intrusion detection system (NIDS) or locally to a host machine as a host-based intrusion detection system (HIDS).

One special method for detecting and examining attacks is a honeypot. Honeypots are decoy establishments for attackers and it's function is to lure attackers into interacting and gather information on malicious behavior targeting the system. Honeypots can be used either to investigate attacks or to act as alarms for ongoing attacks.

For a complex SoS, such as ePilotage, encryption plays essential part in securing traffic between constituent systems. This increases the confidentiality of the messages but also challenges the detection of illicit encrypted traffic. An IDS offers a tool for supervising large networks and for detecting attacks if the challenges caused by encryption are overcome. Honeypots would create an additional layer of security in ePilotage as alerting tools. Honeypots could also create new understanding of fairway cyber risks if used for research purposes.

3.4.1 Case Study: Intrusion detection systems in encrypted traffic (PI)

RQ2: How does increased encryption affect detection of attacks?

Publication PI surveys publications on the topic of detecting intrusions from encrypted traffic. Encryption hinders the functioning of IDSs that rely on inspecting the payload of the traffic. This can be overcome by giving decryption keys to the IDS to enable it to decrypt traffic before inspection. However, sharing decryption keys is not possible or encouraged in every network. It may cause concerns for privacy violations, and interrupting end-to-end encryption may provide attackers an additional access point if the security of the IDS is compromised.

Another option is to analyze the traffic without decrypting it by using traffic analysis methods. These methods function by finding features that characterize normal traffic and then finding traffic whose features form an anomaly. Often, machine learning algorithms are utilized with features related to the timing or the size of the network flow. The more easily definable normal traffic, the more accurate the detection of anomalies. The detection capability is lower than with signature-based solutions, but an IDS can be deployed more freely without the concerns related to decryption key sharing.

According to the surveyed research, the traffic analysis approach is suitable for detecting DoS, brute-force, or scanning attacks that generate a lot of traffic. Detection of subtler attacks, such as injections, has been examined less. In a few papers, detecting more evasive attacks required a preceding phase of more noisy attack types.

For ePilotage, deploying IDSs presents several challenges. The network consists of multiple organizations, systems, and trust zones. Encrypting traffic provides an additional layer of security, but sharing decryption keys is not possible everywhere. Therefore, an alternative option is required. An anomaly detection-based IDS might be a solution, especially for sensor information that consists of a standard type of messaging. This would require more research on the topic. An IDS is only one part of the solution offering information to support security specialists in their work.

3.4.2 Case Study: Honeypot utilization for network intrusion detection (PIII)

RQ3: What type of attacks are detected with honeypots?

Publication PIII presents the use of different types of honeypots and the results of an experiment conducted with Kippo honeypot software. Honeypots are files, software, or devices that are not intended to be found or accessed by legitimate users. Therefore, any access is abnormal and possibly malicious. Honeypots can be used as a research instrument to study the actions of attackers more closely or merely as alerts in the production environment where access triggers a warning. The properties and use case of honeypots vary greatly depending on the intended function and environment.

In the experiment, Kippo honeypot software was used to present itself as a functional SSH server. One honeypot, named Kippo1, was used only to record attempted login credentials, and one honeypot, Kippo2, was set to accept a few selected credentials and to record attacker actions after login. Both honeypots experienced constant login attempts mostly consisting of basic dictionary credentials, for example, "root/root" or "root/123456".

The number and timing of the attempts show that automated attacks, such as botnets, were behind most of the dictionary attack activity. The Kippo2 successful logins revealed that 22 % of IP addresses were able to log in correctly with their first attempt. This suggests that the dictionary attack results were utilized from a different part of the attacker infrastructure. The third part of this infrastructure comprised malware servers from which malware droppers attempted to download content after a successful login. The malware binaries were compiled for several different architectures, including MIPS and ARM, enabling use on, for example, mobile or smart devices.

For ePilotage, the benefits of this study include general visibility of cyber-attackers' basic toolbox. Most of the attempts were made by bots using very common dictionary attacks. For every internet-connected service or device, the attack was averted with strong password policies. The benefits of connecting to the internet should be evaluated, and the resources the login attempts require from the target device should be considered. The malware analysis showed that not only traditional ICT environments are targeted. This means that protection of whole ePilotage environment is important even against generic attacks.

The use of honeypots in the ePilotage environment could increase knowledge of maritime environment cyber activities, and whether they differ from other investigated environments. This would enable more detailed cybersecurity measures. Moreover, honeypots could be used to produce alerts. However, honeypots must be securely implemented so that they do not produce unintended access points for attackers.

3.5 Threats to and vulnerabilities of the ePilotage system

The challenges in understanding cyber threats in ePilotage come from the complexity of the system and the novelty of the topic. To overcome the challenges, the basic elements of cybersecurity in ePilotage must be understood. Publication PIV addresses this topic. One of the most complex entities in the ePilotage environment is the ship. It also presents a notable risk of physical damage if an attack succeeds. The cybersecurity aspect of a ship in ePilotage is investigated in publication PVI. To understand the effects of attacks and related risks, the impacts of cyber-attacks are analyzed in publication PV. However, impacts alone do not provide adequate knowledge of cyber-threat for ePilotage developers. Therefore, adversary profiles are examined, and attack scenarios based on those profiles are created in publication PVII. The rest of the chapter focuses on these publications and their results.

3.5.1 Analysis of cybersecurity of ships in the remote pilotage environment (PVI)

RQ7: How to estimate cyber risk in the complex modern ship environment?

Digitalization and automation have increased in ships and bring an increased number of networks and devices using the networks' access points. In this environment, attacks propagate with lateral movement from device to device until the target is reached. Some attacks require compromise of all sub-assets before advancing, and others need only one previous compromise to advance. The risks can be estimated with a Threats and Risks table (Hummelholm, 2019) which combines information on assets, threats with their risks and existing control mechanisms, risk levels, and decisions on how to react. The table also states recommendations, residual risk levels, and checkpoint options. This table acts as a structured means of gathering the threats to and risks of a network for a unified picture of the situation. The table can be used, for example, in audit and inspection situations or in collaboration to share information. In publication PVI, only an example of this table is presented due to size issues and the unfinished design of ePilotage.

Publication PVI presents an attack tree–based model to evaluate cyber-attack probabilities in a ship's system. This model accumulates attack probabilities over different attack paths in the system but also considers detection mechanisms and countermeasures by reducing the overall success probability. When the probability estimation is taken further, there are multiple attacks against an asset which enable direct attacks or attacks through compromised sub-assets. The probability estimation can be used to track most relevant attack paths through a system.

Publication PVI also discusses the collaboration between constituent organizations of ePilotage. The Observe-Orient-Decide Act (OODA) loop (Boyd, 1996) is suggested for the basis of decision making in complex environments consisting of multiple stakeholders. An audit process by authorities to evaluate the results gained from the ePilotage risk presentation is strongly recommended.

The publication PVI presents attack propagations in an attack-tree based model. However, the equations of attack success probability accumulation need to be corrected in future work. There is a flaw in them, which allows probability to exceed 100 %. While there are multiple different attack possibilities and attack paths, there are also restricting dependencies between different attack paths, for example one failed attack can cause investigation where another, otherwise successful, attack is revealed. The model does not describe this type of features adequately. Future research is needed to formulate attack success probabilities mathematically. The original purpose was to combine situational awareness information throughout the system with boolean algebra and to describe alert's characteristic with numeric value. The attack success probability will need to be separated from this situational awareness alerting and the dependencies between different attack paths need to be studied further to be able to describe the true success accumulation process. This will be considered as future work in the research project.

Another future aspect is assigning numerical values to attack trees. One future tool for this is audit process of ePilotage, where the attack trees are finished and evaluated. In this process, the dependencies, risk- and threat analysis are conducted to ship systems using experts for devices and connections. This process needs iterative approach to find all the relevant characteristics of the system. However, completing an audit process does not mean discovering everything than can ever threaten the system. It merely gives a starting point for the security staff to start working. Eventually, historical data of security events will accumulate creating a basis for more concrete modeling.

3.5.2 Evaluation of the impact of cyber threat in the ePilotage system of systems (PV)

RQ6: What are the impacts of cyber-attacks in ePilotage?

The challenge in this question is the novelty of the environment. No historical data are available, and the ePilotage environment is not available for evaluation. The approach chosen is to analyze impacts that are reported in other cybersecurity contexts and to map them against the basic building blocks of the ePilotage environment defined in publication PIV.

This analysis could have been performed at different abstraction levels. The often-used CIA categorization is one option for evaluating impacts. However, this type of evaluation often is limited in finding more interesting results that come from a more detailed description. Mitre's ATT&CK was chosen as the appropriate abstraction level suited to a system that has no detailed technological information available. Moreover, ATT&CK can address ICT and ICS aspects of attacks. The impacts are listed in Table 1. The analysis of the whole attack path would have been too hypothetical; therefore, the focus is on the results of an attack, and not on the methods with whom those results were achieved. The evaluation supports risk evaluation because it describes the impact portion of cyber-attacks in ePilotage. Both ICT and ICS impacts did provide meaningful interpretations in ePilotage context. Especially, considering ICS aspects proved to be valuable for the CPS side of ePilotage.

Table 1 ATT&CK impacts (PV).

ICT environment impacts	
	Account Access Removal
	Data Destruction
	Data Encrypted for Impact
	Data Manipulation
	Defacement
	Disk Wipe
	Endpoint Denial of Service
	Firmware Corruption
	Inhibit System Recovery
	Network Denial of Service
	Resource Hijacking
	Service Stop
	System Shutdown/Reboot
ICS environment impacts	
	Damage to Property
	Denial of Control
	Denial of View
	Loss of Availability
	Loss of Control
	Loss of Productivity and Revenue
	Loss of Safety
	Loss of View
	Manipulation of Control
	Manipulation of View
	Theft of Operational Information

Special characteristic arising from the SoS aspect of ePilotage was the propagation of attack effects from one constituent system to another. Dependencies for correct and timely information are critical points of failure. These dependencies did not stay withing one constrained environment. They were forming between different constituent systems and did also include connections between ICT and ICS environments. CPS aspect of ePilotage was seen well when considering the ICS impacts from ATT&CK. The impacts transformed from data related effects to destruction of physical assets such as ships. Time criticality in detecting, deciding, and acting was the result of more constrained safe operating space of piloted waters.

When reflecting the results to documented attacks, and exploitation demonstrations, the results prove be accurate. The live attacks enrich the view of how the attacks can be performed but the framework is able to describe them. Using the framework add the benefit of considering all the attack options in more controlled fashion and not just the most recent ones or the ones that have gained the most headline space.

3.5.3 Analysis of cyber threats in the remote pilotage system (PVII)

RQ8: What are the characteristics of cyber threats to ePilotage?
RQ9: How to create cyber-attack scenarios for ePilotage?

As noted previously in the thesis, cyber threats are not defined consistently or analyzed in a unified manner. In this thesis, a cyber threat consists of the actors and their actions, as a threat is seen to consist of intent, opportunity, and capability (figure 4). The actor side defines the motivations that create intent, clarifies the opportunities used, and creates restrictions for the available capabilities. The actions side defines the attack techniques which are included in the actor's capability set.

A cyber threat is not a static phenomenon but evolves constantly. Therefore, an evolving set of attacks is employed to enable the usability of the method in the future as well. Another benefit ATT&CK offers is that it lists mitigation methods for each attack. In publication PVII, attacks and their mitigation methods are listed for the created scenarios. This reveals the type of actions to which the design process responds to.

As a result, publication PVII presents archetypes of attackers against the ePilotage environment, and from these archetypes, attacks are induced with the aid of the ATT&CK framework and the ePilotage design. Additionally, the relevance of up-to-date cyber awareness is demonstrated by utilizing trend reports and recent malware sightings. This creates scenarios that demonstrate attacks through believable motivation, tools, and techniques.

As a disadvantage, this approach may neglect unique attack approaches that utilize zero days or attack techniques not yet discovered. However, as a starting point, the likely attack scenarios offer solid ground to start the building process. More advanced scenarios may be created later after the basic security establishments are in good order.

Evaluating mitigation options is a bonus effect offered by the use of ATT&CK. When the scenario is created, the mitigation options can be evaluated separately. Security training for staff was one of the mitigation recommendations that was found by analyzing scenarios. In addition, the related research section in publication PVII it was found that cybersecurity awareness in the maritime sector is not as high as it could be. Therefore, this mitigation recommendation should not be taken lightly. The mindset of correct behavior must be introduced to the field, because technological barriers alone are not enough to stop the adversary.

3.6 Conclusions

One of the design challenges of ePilotage is how to incorporate current pilotage practices and environments as transforming vessels will take time. Currently, many aspects in pilotage design do not support security aspects of CIA.

ICS cybersecurity aspects offer promising results for ePilotage's need for describe cybersecurity issues also outside the traditional ICT focus. At the minimum, when the ICS is not seen only for industrial settings but covers larger nontraditional embedded solutions and sensor networks.

Another challenging aspect of ePilotage arises from the complexity of the whole. The single constituent system of a ship is complex as well as the combination of all the stakeholder systems. This creates propagation paths for attacks to advance from the weakest link in the SoS to others. Detecting attacks and understanding the link between the steps in different systems require more research and thorough consideration from system developers to create detection and communication networks that cover more than one part.

In evaluating possible cyber-attacks on ePilotage, propagation of attacks in the SoS should be considered. The MSMS can be utilized to create comprehensive scenarios. This can be done, for example, by including the human aspect (reaction to phishing), processes (how to communicate ongoing technical disturbances), and technology aspects (vulnerabilities to malware infections) as the attack propagates through multiple systems.

As demonstrated in PV and PVII, ATT&CK is capable to act as a framework to describe and to help create understanding of cyber threat in ePilotage. The SoS and CPS aspects need to be considered by ePilotage experts, but the framework is able to support this process. What is needed more is the attacker archetype description to focus the analysis efforts and the information sources describing latest innovations and trend developments in the field.

The reflect the results on the role of cyber threats in risk evaluation (depicted in figure 4), it can be seen that the archetype information is responsible for intent and restricts the capabilities selection options. Archetypes also relate to the opportunity types the attacker wishes to use. Capabilities and impacts are described by ATT&CK frameworks. Vulnerabilities in deep technological level are the vulnerabilities of the used systems and these will change over time. This also is highly dependent on the technological choices in the environment. Some of the vulnerabilities of the current maritime environment were discovered and likely some of these will be present in the ePilotage environment due to slow update possibilities throughout the entire maritime transportation ecosystem. However, the analysis provided ePilotage specific vulnerabilities related to the

SoS structure and the time criticality. The dependencies and data flow trust issues can be discovered and addressed in the design process of ePilotage.

The most restricting issue currently is the lack of maritime specific cyber threat information. It was demonstrated that the existing frameworks can be utilized in describing the cyber threat and in evaluating risks, but more information is required to see the maritime specific trends. This needs the cooperation of the maritime industry with the cyber security community.

4 CONCLUSIONS AND DISCUSSION

4.1 Introduction

This dissertation has two perspectives, theoretical and practical. They are discussed separately. Then, the reliability and validity of the results are presented. The limitations of this doctoral dissertation are discussed before recommendations for further research are provided.

4.2 Theoretical implications

4.2.1 Examination of cyber threats and detection

RQ1: What type of cyber-attacks have occurred in critical infrastructure? (PII)

Cyber-attacks in the energy sector present examples of cyber threats in critical infrastructure. Attacks vary widely from collateral damage to highly advanced targeted campaigns.

RQ2: How does increased encryption affect detection of attacks? (PI)

Encryption restricts the deployment of detection mechanisms that rely on inspection of clear text messages. However, traffic flow features enable the detection of some types of attacks, especially those that cause increased network traffic. These detection mechanisms can use machine learning methods with high detection rates and accuracy. Detection of covert attacks by machine learning has not been investigated extensively, and successful detection of these attacks is uncertain. For this type of attack, other methods are required. One option is to set an IDS with a decryption key to inspect traffic. However, in this case the IDS will create a single point of failure. If it is compromised, all encrypted traffic the key is capable of decrypting will be revealed to the attacker.

RQ3: What type of attacks are detected with honeypots? (PIII)

Honeypots enable defensive and research approaches. For production environments, a low-interaction honeypot can act as a supplementary method for detecting attacks and sound an alarm if it detects an attack. However, relying only on honeypots is not applicable as an attack can leave a honeypot untouched. For the research approach, a honeypot deployed in a fairway setting might provide unique information on attacks specific to this environment. As confirmed attacks and their details are not widely available, the information that a honeypot could provide would be very useful.

The deployment of an SSH honeypot revealed that environments other than traditional ICTs are targeted. For ePilotage, this result emphasizes the need to secure ICT and ICS environments.

4.2.2 The ePilotage environment and cyber threats

RQ4: What does the ePilotage environment consist of?

ePilotage's constituent systems include ships, the fairway, and the control center as the main systems. Support systems include VTS, weather forecasting, other vessels, and stakeholders' operators. This network forms a system of systems, but as these constituent systems have their own outside dependencies, the picture becomes far more complex. For example, the ship has its own systems that are linked to the owner's systems and the technology providers' processes. Supply chains reach far outside the core ePilotage system and create possible attack paths.

RQ5: What are the cybersecurity elements of ePilotage?

The cybersecurity elements consist of understanding the aspects and their connections. These are presented in the Maritime Security Management System for ePiloting in publication PIV. This includes activities, stakeholders, organizational relationships, security dimensions, security elements, and criteria. The variety of elements emphasizes that security is not just technical issue but also encompasses systems, humans, and interactions. All of this can be viewed through different levels of abstraction. This thesis is only a small portion of this entire picture, and further work must be done.

RQ6: What are the impacts of cyber-attacks in ePilotage?

The unique features of ePilotage include a strong CPS presence and a limited timeframe for defensive actions. These features manifest in worst-case scenarios where data loss is not the most dire result of a successful attack. Loss of life is possible when the control of a large physical element like a ship is lost to a malicious attacker. In a fairway environment, the physical proximity of the shore and other vessels restricts the time until a ship will collide if something is wrong.

The number of constituent systems introduces an element of attack propagation through systems. It is easier to detect if a system is not functioning than to detect altered information. If a system fails due to a breakdown in communication or an attack, the failure can be substituted with a backup system. Detecting altered information requires independent additional sensors for the same information and correlating the readings from these sensors. However, the correlation process is not straightforward, as the amount of information and the number of different sensors are likely to increase in the future. A subtle alteration can mimic, for example, weather conditions and stay hidden.

In the SoS environment, the dependencies and responsibilities might be unclear within the organizations, which might delay corrections and timely responses to a cyber-attack. If ePilotage is attacked as a SoS, every organization sees only a portion of the whole situation unless the cooperation is seamless.

RQ7: How to estimate cyber risks in the complex modern ship environment?

A modern ship is a complex entity due to its connected systems. Publication PVI presents tools for organizing assets, related threats, and their propagation. Assets, threats, countermeasures, and associated risk levels can be collected in a table and the table used in the audit process. The propagation of risk can be evaluated through formulas for the accumulation of common risk probabilities presented in publication PVI. In the calculation, it is important to notice that an asset may be compromised through a sub-asset or by a direct attack. There may be multiple attacks against one asset with different success probabilities. Countermeasures and detection capabilities decrease success probabilities. These probabilities are to clarify the most vulnerable aspects of a ship.

RQ8: What are the characteristics of cyber threats to ePilotage?

Not all cyber-attacks are the same. Evaluating every possibility of everything creates a massive task that may be possible once, but keeping the information and process up to date is unlikely.

Attacker archetypes create the first opportunity to limit the number of likely events by recognizing that different attackers aim for different outcomes with different capabilities. The use of capabilities can be estimated from databases that contain attack information, such as ATT&CK or trend reports. This information changes more often than the original archetypes, and therefore, a fixed set of attacks is either highly abstract or unable to describe currently active attacks.

From the technological perspective, ePilotage has significantly more ICS and sensor components than the traditional ICT environment. The ICS presence challenges security teams but also demands more capabilities from attackers if they target the ICS environment. Attacks propagating from the ICT environment to the ICS or vice versa will challenge security teams.

RQ9: How to create cyber-attack scenarios for ePilotage?

Cyber-attack scenarios can be created even for an environment that does not have established technologies. This affects the level of detail available.

However, some things can be seen from related research and other publications. By first considering the cyber-threat actor, a model of generic behavior can be created. This includes motivation and capabilities. By understanding the behavior, higher risk situations can be evaluated. These situations include societal and national events more broadly. For example, a strike at a port might have cyber-related consequences. From the capabilities of an actor, a proper approach level can be estimated. A generic crime does not necessarily include a targeted multifaceted attack against the entire ePilotage, but a nation-state actor might include zero-day malware in its campaign. The usual methods of attacks can be seen from attack databases and trend reports. Possible future attacks can be estimated from attack demonstrations and academic proof-of-concept papers. Combining these sources with the attacker profile and ePilotage environment information creates scenarios that are credible. The scenarios can be utilized in system design, development, and training purposes. They need to be re-evaluated and evolve regularly as the cyber scene is ever changing.

4.3 Practical implications

From the answers to research questions, it can be seen, that there are risks related to intentional harmful actions against ePilotage in the cyber domain and technological vulnerabilities that increase this cyber-risk. Focusing on safety issues only is not enough to mitigate cyber-attacks. Therefore, cybersecurity professionals should be included in the design process to evaluate cyber-threat and vulnerabilities, and to enhance risk evaluation with cybersecurity aspect.

For a vast and complex SoS, such as ePilotage, it is important to create a clear understanding of all the aspects that affect the system's cybersecurity. As the attacks propagate from system to system, the systems' connections, data flows, and technologies with associated vulnerabilities must be known.

Because of the connections between constituent systems a large attack campaign might attack ePilotage as a whole instead of single systems. Therefore, there should be some entity responsible for the cybersecurity aspect of whole ePilotage and the constituent organizations should plan together how to react to cyber-attacks. There will not be one instance dealing with all the security aspects, as the constituent systems are operated by different organizations. However, someone must set the requirements and oversee that they are met. Creating the requirements is a difficult task considering the heterogeneity, for example, in ship types, and the life span of systems is long, making updates sometimes challenging.

Cybersecurity challenge does not end with the completion of design phase. As cyber-threat evolves, ePilotage needs to adapt. Knowledge on cyber-threat evolution and the effects on cyber-risk levels need to be considered regularly and integrated into the general risk management procedures. In addition, the knowledge needs to be shared among constituent organizations for actions such as training and system management.

4.4 Reliability and validity

This dissertation presents a case study concerning one environment which is in its early design phase. It can be seen that some ship technologies will exist for a long period. These include well-established and partly mandatory elements of the AIS, ECDIS, and GNSS. For other parts of the ePilotage environment, the attack elements will function as the first phase of evaluation before more data are acquired. The suggested scenarios should be re-evaluated when new information on attacks or technologies is discovered.

The issues found in the ePilotage environment are partly applicable to other critical infrastructure fields. Of course, mandatory technologies are different outside the maritime environment, and the tolerance for error varies. Depending on the environment, the severity of the impacts may vary. However, the scenario creation based on attacker archetypes, attack information, and frameworks is suitable when tailored to the target environment. A framework similar to the MSMS can be used in gathering the key aspects of the target system's features, and using ATT&CK provides a flexible information base for different types of environments. The challenges of outdated systems and complex dependencies may concern many other CI fields, especially those that utilize embedded and/or specialized software that resembles ECDIS, for example. If these data are also widely available online (resembling AIS information), effects similar to those in the maritime environment can be seen.

4.5 Limitations of the doctoral dissertation

This doctoral dissertation offers one piece for solving the puzzle of ePilotage design. However, situations change constantly, and the knowledge provided can be seen only as a starting point in the constant evaluation of cyber threats. Even this thesis might alter the situation, as it sets scenarios for defending the SoS. A capable adversary will take note and will find an alternative route.

This doctoral dissertation is based on public information and articles. Therefore, the technical description and defense mechanisms of the ePilotage environment may be different than assumed. This limitation must be considered when using the cyber-threat descriptions and scenarios. Accommodating more accurate design information in cyber-threat descriptions is highly recommended for more effective results. However, the basic concept of generating scenarios based on adversary and attack information is valid.

4.6 Recommendations for further research

One of the major limitations for this thesis was the availability of information. Making information about maritime cyber-attacks, system vulnerabilities, and attackers specialized in the maritime environment more widely available is vital for accurate design and defense. Examples include deploying a honeypot for the maritime environment or conducting vulnerability scans of systems in use.

Completing a thorough risk-assessment process for ePilotage requires more information on the specific chosen technologies and their vulnerabilities. This would create a more complete picture of the cyber-risk situation, as actual vulnerabilities could reveal previously undiscovered attack paths. Moreover, the scenarios presented should be evaluated against the design of ePilotage and more detailed scenarios developed based on the detailed environment.

YHTEENVETO (SUMMARY IN FINNISH)

Väitöksessä käsitellään etäpilotoinnin kyberturvallisuuden toteuttamista erityisesti kyberuhkaa analysoimalla. Väitökseen sisältyy seitsemän vertaisarvioitua julkaisua, jotka käsittelevät väitöksen aihekokonaisuuden eri osioita. Tuloksena esitetään kyberuhkamalli, joka koostuu uhkatoimijoiden arkkityyppien kuvauksista, sekä näiden pohjalta luotujen skenaarioiden rakentaminen käyttäen kyberturvallisuusyhteisön ylläpitämää hyökkäystietokantaa. Tulevaisuuden työksi nähdään holistisen riskiarvioinnin toteuttaminen yhdistämällä väitöksen uhkatieto haavoittuvuustietoihin, joita on mahdollista analysoida tarkemmin vasta ympäristön teknisten kuvausten ollessa pidemmällä. Lisäksi luotuja skenaarioita tulee päivittää päivittyvän tietämyksen myötä ja käyttää suunnitteluprosessin apuna testaamaan ympäristön kybersietoisuutta.

REFERENCES

Ahvenjärvi, S. (2016). The human element and autonomous ships. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 10*(3), 517-521.

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia, 45,* 547-554.

Alexander, O., Belisle, M., & Steele, J. (2020). Mitre ATT&CK® for Industrial Control Systems: Design and Philosophy.

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, 1-8.

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The Impact of Control Technology, 12*(1), 161-166.

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. In *Proceedings of the 30th Annual Computer Security Applications Conference* (ACSAC '14). Association for Computing Machinery, New York, NY, USA, 436–445.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security, 89,* 101677.

Bhatti, J., & Humphreys, T. E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. *NAVIGATION: Journal of the Institute of Navigation, 64*(1), 51-66.

Bimco. (2020). The guidelines on cyber security onboard ships - Version 4, [online], https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

Bodeau, D., & Graubart, R. (2017). *Cyber Prep 2.0 Motivating Organizational Cyber Strategies in Terms of Preparedness*. Bedford, MA: Mitre Corp.

Bodeau, D. J., & McCollum, C. D. (2018). *System-of-Systems Threat Model*. McClean, VA: Mitre Corp.

Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). *Cyber Threat Modeling: Survey, Assessment, and Representative Framework*. McClean, VA: Mitre Corp.

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science, 131,* 104908.

Boyd, J. R. (1996). *The Essence of Winning and Losing*. Unpublished lecture notes.

Casey, T. (2015). Understanding cyber threat motivations to improve defense. Intel white paper.

Council of the European Union. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union. [online], https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G. B., & Wyss, G. (2005). Risk assessment for physical and cyber attacks on critical infrastructures. In Proc. IEEE MILCOM, Oct. 17–20, 2005, vol. 3, pp. 1961–1969.

DIMECC. (2020). Sea for Value (S4V). [online], https://www.dimecc.com/dimecc-services/s4v/

European Commission. (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protection, Brussels, 12.12.2006 COM(2006) 786 final. [online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

European Union Agency for Cybersecurity. (2011). Analysis of cyber security aspects in the maritime sector. [online], https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

European Union Agency for Cybersecurity. (2019). Port cybersecurity: Good practices for cybersecurity in the maritime sector.

Finlex. (2021). Luotsauslaki, ajantasainen lainsäädäntö, [online], https://www.finlex.fi/fi/laki/ajantasa/2003/20030940.

Fintraffic. (2021). Fintraffic´s Vessel Traffic Services – safe maritime traffic, [online], https://www.fintraffic.fi/en/vts.

Fireeye. (2021). *M-Trends 2021, Annual Threat Report*, [online], https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

Fox, D. B., Arnoth, E. I., Skorupka, C. W., McCollum, C. D., & Bodeau, D. J. (2018). *Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions: Threat Model ATT and CK/CAPEC Version*. McClean, VA; Mitre Corp.

Guo, Y., Lou, X., Bajramovic, E., & Waedt, K. (2020). Cybersecurity risk analysis and technical defense architecture: Research of ICS in nuclear power plant construction stage. In *Proceedings of the 3rd IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts* (ICONS 2020).

Hummelholm, A. (2019). *Cyber Security and Energy Efficiency in the Infrastructures of Smart Societies*. Jyväskylä: University of Jyväskylä.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80.

International Association of Marine Aids to Navigation and Lighthouse Authorities. (2004). IALA Guideline No. 1028: On the Automatic Identification (AIS) Volume 1, Part I Operational Issues, Edition 1.3, [online], https://www.navcen.uscg.gov/pdf/AIS/IALA_AIS_Guidelines_Vol1_Pt1%20OPS%20(1.3).pdf.

International Association of Marine Aids to Navigation and Lighthouse Authorities. (2007). IALA Recommendation A-126, On the use of the Automatic Identification System (AIS) in Marine Aids to Navigation

Services, Edition 1.3, June 2007, [online], https://www.navcen.uscg.gov/pdf/AIS/IALA_A126_AIS_ATON%20(1.3).pdf.

International Maritime Organization. (2017). Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3, 5July2017, [online] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

ITU-T. (2008). ITU-T X.1205 Overview of cybersecurity, Series X: Data networks, open system communications and security..

Tam, K., Jones, K. D., & Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. *Eng. Technol. Ref, 1*(5pp), 1-13.

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2018). Cyber-attacks against the autonomous ship. In *Computer Security* (pp. 20-36). Cham: Springer.

Kongsberg. (2020). Kongsberg Maritime and Massterly to equip and operate two zero-emission autonomous vessels for ASKO, [online], https://www.kongsberg.com/newsandmedia/news-archive/20202/zero-emission-autonomous-vessels/.

Kooij, C., Colling, A. P., & Benson, C. L. (2019). When will autonomous ships arrive? A technological forecasting perspective. In *Proceedings of the International Naval Engineering Conference and Exhibition (INEC).*

Lahtinen, J., Banda, O. A. V., Kujala, P., & Hirdaris, S. (2020). The risks of remote pilotage in an intelligent fairway–Preliminary considerations. In *Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC) 2019* (pp. 48-57). Sciendo.

Lehto, M. (2020). Phenomena and Definitions of the Digital Cyber World, unpublished research report, University of Jyväskylä.

Lehto, M., & Neittaanmäki, P. (2018). *The Modern Strategies in the Cyber Warfare. Cyber Security: Cyber Power and Technology*. Berlin: Springer.

Levin, T. (2020). IBM will send an autonomous research vessel across the Atlantic next year, [online], https://www.businessinsider.com/ibm-transatlantic-autonomous-research-vessel-ship-across-atlantic-ocean-mayflower-2020-9?r=US&IR=T.

Libicki, M. C. (2007). *Conquest in Cyberspace – National Security and Information Warfare.* New York: Cambridge University Press.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6, 9*(1-2), 3-31.

Lukka, K. (2003). The constructive research approach. Case study research in logistics. *Publications of the Turku School of Economics and Business Administration, Series B, 1*(2003), 83-101.

MarineTraffic. (2021). Marine Traffic: Global ship tracking intelligence, AIS Marine Traffic, [online], https://www.marinetraffic.com

Massterly. (2021). What we do, [online], https://www.massterly.com/what-we-do.

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 91-98). Location: IEEE.

Medina, D., Lass, C., Marcos, E. P., Ziebold, R., Closas, P., & García, J. (2019, July). On GNSS jamming threat from the maritime navigation perspective. In *22nd International Conference on Information Fusion* (FUSION) (pp. 1-7). Location: IEEE.

Meyer, C. B. (2001). A case in case study methodology. *Field Methods*, *13*(4), 329-352.

Nielsen, C. B., Larsen, P. G., Fitzgerald, J., Woodcock, J., & Peleska, J. (2015). Systems of systems engineering: basic concepts, model-based techniques, and research directions. *ACM Computing Surveys (CSUR), 48*(2), 1-41.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version, 1.1, [online], https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Obregon, L. (2015). Secure architecture for industrial control systems. *SANS Institute InfoSec Reading Room*.

Perro, C. (2001). Accidents, Normal. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 33-38). https://doi.org/10.1016/B0-08-043076-7/04509-5.

Ponemon Institute. (2018). *Study on Global Megatrends in Cybersecurity*. Research Report: Location: Ponemon Institute.

Pöyhönen, J., & Lehto, M. (2020). Cyber security: Trust-based architecture in the management of an organization security. In *The 18th European Conference on Cyber Warfare and Security ECCWS2020* (pp. 304-313).

Rolls-Royce. (2018). Rolls-Royce and Finferries demonstrate world's first fully autonomous ferry, [online], https://www.rolls-royce.com/media/press-releases/2018/03-12-2018-rr-and-finferries-demonstrate-worlds-first-fully-autonomous-ferry.aspx.

Rødseth, Ø. J., & Nordahl, H. (2017). *Definition of Autonomy Levels for Merchant Ships*. Report from NFAS, Norwegian Forum for Autonomous Ships, 2017-08-04.

Rushby, J. (1994). Critical system properties: Survey and taxonomy. *Reliability Engineering & System Safety*, *43*(2), 189-219.

Secretariat of the Security Committee. (2013). Finland's Cyber Security Strategy, Government Resolution 24.1.2013.

Son, P. W., Park, S. G., Han, Y., & Seo, K. (2020). eLoran: Resilient positioning, navigation, and timing infrastructure in maritime areas. *IEEE Access, 8,* 193708-193716.

Statista Reseach Department. (2020). Age distribution of world merchant fleet by vessel type 2019-2020. [online]

https://www.statista.com/statistics/1102442/age-of-world-merchant-fleet-by-vessel-type/

Stouffer, K., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security, revision 2. *NIST Special Publication, 800*-82.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. Technical report.

Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of Maritime Affairs, 18*(3), 509-520.

Tam, K., & Jones, K. (2019a). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs, 18*(1), 129-163.

Tam, K., & Jones, K. D. (2019b). Situational awareness: Examining factors that affect cyber-risks in the maritime sector. International Journal on Cyber Situational Awareness, 4(1), 40-68.doi:10.22619/IJCSA.2019.100125

Thai, V. V., & Grewal, D. (2007). The maritime security management system: Perceptions of the international shipping community. *Maritime Economics & Logistics*, 9(2), 119-137.

The Maritime Safety Committee. (1998). Resolution MSC.74(69), Adoption of new and amended performance standards, [online], https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.74(69).pdf.

The Maritime Safety Committee. (2010). Resolution MSC.308(88) (adopted on 3 December 2010), Amendments to the international convention for the safety of life at sea, 1974, AS AMENDED, [online], https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.308(88).pdf

The Maritime Safety Committee. (2017). Maritime cyber risk management in safety management systems, Resolution MSC.428(98), [online], https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Tulli. (2020). Ulkomaankaupan kuljetukset 2019, [online], https://tulli.fi/-/ulkomaankaupan-kuljetukset-vuonna-2019.

United Nations Conference on Trade and Development. (2020). *Review of maritime transport 2020*. New York: United Nations.

Vesselfinder. (2021). Free AIS ship tracking of marine traffic, [online], https://www.vesselfinder.com/

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38,* 97-102.

Xiong, W., & Lagerström, R. (2019). Threat modeling—A systematic literature review. *Computers & Security*, *84*, 53-69.

Yara. (2020). Yara Birkeland status, [online], https://www.yara.com/news-and-media/press-kits/yara-birkeland-press-kit/.

ORIGINAL PAPERS

I

SURVEY: INTRUSION DETECTION SYSTEMS IN ENCRYPTED TRAFFIC

by

Kovanen, T., David, G., & Hämäläinen, T., 2016

In O. Galinina, S. Balandin, & Y. Koucheryavy (Eds.), Internet of Things, Smart
Spaces, and Next Generation Networks and Systems (pp. 281-293). Springer
International Publishing.

DOI: 10.1007/978-3-319-46301-8_23

Reproduced with kind permission by Springer.

Survey: Intrusion detection systems in encrypted traffic

Tiina Kovanen, Gil David, Timo Hämäläinen

University of Jyväskylä, Jyväskylä, Finland

{tiina.r.j.kovanen, gil.david, timo.t.hamalainen}@jyu.fi

Abstract. Intrusion detection system, IDS, traditionally inspects the payload information of packets. This approach is not valid in encrypted traffic as the payload information is not available. There are two approaches, with different detection capabilities, to overcome the challenges of encryption: traffic decryption or traffic analysis. This paper presents a comprehensive survey of the research related to the IDSs in encrypted traffic. The focus is on traffic analysis, which does not need traffic decryption. One of the major limitations of the surveyed researches is that most of them are concentrating in detecting the same limited type of attacks, such as brute force or scanning attacks. Both the security enhancements to be derived from using the IDS and the security challenges introduced by the encrypted traffic are discussed. By categorizing the existing work, a set of conclusions and proposals for future research directions are presented.

Keywords: Intrusion detection system, encrypted traffic, traffic analysis

1 Basics of Intrusion Detection Systems

Intrusion detection system, IDS, is used to examine network traffic and to detect malicious activities. One classification basis of IDSs is the location of the sensor. It can be local on the protected machine or reside at some point in the network protecting a larger group of machines. The local IDS is known as Host-based Intrusion Detection System, HIDS, and the one residing in the network is Network Intrusion Detection System, NIDS. As for encrypted traffic IDS, it is easier for a HIDS to have the encryption keys and thus be able to analyze decrypted data. On the other hand, HIDS is unable to detect attacks that spread in the network as the HIDS is limited to the local view. Another security tool to be noted is application firewall which has similar detection capabilities as an IDS. Encryption is a challenge that is often dealt with by sharing decryption keys.

Another way to classify IDS is based on the attack detection methodology. Usually IDSs are separated into two different categories, signature based or anomaly detection based (see e.g. [1]). Signature based detection is done by inspecting the payload and comparing the findings to known attacks. This method is generic since the same signatures should apply to any known network. Signature based method is accurate for known attacks, but is unable to handle new threats. Anomaly detection based method compares the traffic to known normal traffic patterns and if big enough deviation is detected, the traffic is classified as malicious. This method is less generic since it adapts the normal traffic model to the learnt network, thus providing an adaptive model that captures the actual behavior. Anomaly detection based methods are less accurate than signature based methods but they are able to detect new types of attacks also called as zero-day attacks.

Koch [1] stated that the rise of encrypted traffic is one of the challenges that future IDS have to be able to cope with. As encrypted traffic comes more and more common, the payload inspection becomes less valid approach. Nonetheless malicious activities are still in the networks and need to be detected. There are three different approaches in handling encrypted traffic inspection and all of them have their unique disadvantages [1], [2]. The first one is protocol based detection, but it only detects misuse of encryption protocol itself. Attacks done using an encrypted channel remain unnoticed. The second option modifies network infrastructure and needs decryption. Last option is based on traffic analysis, which extracts information from the traffic flow. In this survey the protocol based detection is included in traffic analysis category if it does not require decryption. This leaves us two categories that are separated by the need for decryption.

As most IDS detection methods rely on inspecting the payload of the messages, traffic decryption becomes a natural solution for encrypted data. This reduces the problems of encrypted traffic IDS back to the traditional challenges of any IDS. Accessing decrypted data can be done by several different methods varying from shared encryption keys to reverse engineering applications. However, requiring decryption has several drawbacks. The first one is obvious, decryption is not possible nor allowed in all network environments. The second one is ethical and has to do with user privacy. The third one is the concern for security. As end-to-end encryption is broken, this gives malicious adversaries another attack point. The third concern is addressed in some publications but none of them can render the first concern obsolete. Thus we have to take a look at what traffic analysis methods can provide.

Traffic analysis methods have the advantage that they do not require decryption. This allows their implementation in all the same places as traditional IDSs. Traffic analysis methods aim to define characteristics of normal network traffic and often focus on the network flow. Different aspects are taken into consideration such as timing and size of the packets. After the features are extracted different anomaly detection and machine learning methods are applied. The major drawback of this approach is a lower detection accuracy than a traditional IDS. This is due to the fact that payload data is encrypted, hence less information is available for the analysis.

Dyer et al. [3] report that encryption protocols such as TLS, SSH and IPsec were all susceptible to traffic analysis attacks. This means that information can be extracted from different kinds of encrypted traffic.

2 Attacks

Encryption of traffic limits heavily the availability of different features in data. Therefore, it is tempting to focus on attacks that presumably are visible through increased traffic. These attacks include scanning, brute force and dictionary attacks and DoS / DDoS. It is shown in many articles that such attacks are visible from network flows [4]. However, detection of other types of attacks in encrypted traffic using methods that do not require decryption is much less studied. To be visible without decryption, the attack needs to fulfill few requirements. Firstly, the detection of attacks is only possible if the traffic goes through the IDS. Some attacks can be locally executed or use alternative route to target. In these cases, IDS cannot detect the direct attack but might detect side effects of the attack. One example of this type of an attack is virus on a USB drive, where the virus activates locally on the machine. On the other hand, some more advanced IDSs are able to detect further stages of the attack such as contacting C&C server and possible exfiltration of files. Secondly, the attack has to change some of the network traffic features. Detection of zero-days attacks and targeted attacks is possible by focusing on the network traffic behavior by modelling various detectable attack features, without relying on known attack signatures. We present a set of detectable attack features in table 1.

Table 1. Detectable attack features.

Detectable attack features
1. **Frequency of sent packets**
2. **Frequency of received packets**
3. **Ratios between sent / received packets**
4. **Ratios between sent / received packet sizes**
5. **Time between sent / received packets**
6. **Number of packets**
7. **Size of packets**
8. **Session duration**
9. **Changed request – reply sequences**
10. **Endpoint identity**
11. **Connection hour and day**
12. **Response time**

IDS has to identify malicious activities that have varying features depending on the phase and type of the attack. According to Engen [5] the phases of the attack can be divided into four sections: surveillance, exploitation, mark and masquerade. The first phase includes scanning and probing activities to gather information of the target system. This phase includes possible password cracking by brute force or dictionary attacks. The second phase includes using suitable exploit to the system to gain access with administrator privileges. This phase may contain Denial of Service (DoS) attacks, which usually try to flood the system with requests so that it is unable to respond. The third phase includes the malicious activity of the attacker in the system. This phase may consist of stealing or destroying data, planting malicious software on the system or using it for other attacks. The last phase involves hiding evidence of successful intrusion. This may be done by deleting activity log entries and removing executed malware files.

Table 2. Attack phases, corresponding attack types and examples.

Phase	Attack type	Examples
Surveillance	Scanning (Targeted)	Targeted against a specific computer or vulnerability
	Scanning (Mass)	Large scale scanning to find any target
	Password cracking	Dictionary or brute force attack
Exploitation	DoS / DDoS flooding type	Server resources are depleted by numerous requests
	DoS / DDoS vulnerability type	Server resources are depleted by targeting known vulnerability
	Remote-to-Local	SQL injection
	User-to-Root	Buffer overflow
	Zero-day attacks	Previously unknown attacks
Mark	Data exfiltration / deletion / alteration	Insider action or after a breach
	Spyware	Keylogger
	Other malware execution	Spying or causing harm
Masquerade	Log entry, malware trace etc. deletion	Possible backdoor left open

Table 2 presents the four phases of an attack according to Engen [5], with corresponding types of attacks and examples. By using a taxonomy for attacks it is easier to cover more different types of attacks. All the attacks that have detectable features might be detectable with traffic analysis. Many of the attack types can belong to several phases depending on the motivation of the attacker. For example, DoS can be seen as an exploitation phase action, where it enables other attack vectors to succeed. It can also be seen as the actual attack belonging to the mark phase. In this case the motivation is just to shut down the target system with no further intentions. Also most of the Mark phase attacks are exploits too but are here seen as the end goal of an attack and thus categorized to Mark phase.

Another aspect is the location of the IDS. This affects, for example, the endpoint identity feature's usability. If the protected machine is a web server, all the connections are accepted unless black listing is used. This means that every endpoint is regarded benign unless an attack is discovered by other means. On the other hand, if the protected machine is in limited network, the approach adds a valuable feature in the case when not all of the machines are allowed to contact each other. This also requires identification of endpoints. If NAT connections are used, simple identification based on IP addresses fails. Also spoofing IP addresses and port information is possible.

3 Literature

During recent years, the percentage of encrypted traffic is constantly increasing, and the number of articles discussing the encrypted traffic IDS domain is increasing respectively. In this survey, we selected research papers that discuss the detection of attacks from encrypted traffic. Snowball search is technique which searches more publications from the citations of referred publications [6]. This was used to retrieve the central citations of the found publications. These citing articles were reviewed by title. The number of found articles was limited but more insight was found from articles discussing traffic analysis attacks and encrypted traffic classification. Also most of the encrypted traffic IDS papers refer to these near field topics as the basis of their own research. The approaches in traffic analysis attacks and encrypted traffic classification research are slightly different than in encrypted traffic IDS but the methods can be useful in all of these research activities.

Traffic analysis attack studies discuss different methods of extracting information from encrypted traffic based on information available without decryption [3], [7]–[9]. The aim is not to the detect intruders but rather to point out that encryption has limitation in hiding sensitive information. For example, revealing the identity of visited web pages in encrypted web traffic is possible without decryption [9]. Encryption protocols use packet padding to obfuscate packet size information and thus attempt to prevent traffic analysis attacks. It is shown that padding encrypted traffic is not enough to prevent traffic analysis attacks [3], [10], [11]. In encrypted traffic IDS the ideas of traffic analysis attacks are used to reveal malicious activities rather than gaining sensitive information from encrypted traffic.

Encrypted traffic classification aims to identify applications sending the encrypted traffic. The research question is not focused in finding malicious activities but aims to produce viable information for quality of service decisions. For example, VoIP calls or SSH connections are identifiable without decryption [12]–[21]. Deep packet inspection and port numbers are not needed to identify various application and protocols. This enables the creation of normal traffic pattern from which the deviations can be detected. However, the results are often too coarse to meet the expectations of traffic managers [19]. The publication on encrypted traffic classification enforce the view that encryption does not hide the typical features of an application. The more information it is possible to gather from encrypted traffic without decryption, the more possible it becomes to detect attacks from the features they have.

3.1 Encrypted traffic IDS

Some of the articles discussing encrypted traffic IDS use an approach that requires decrypting the traffic before IDS analysis is done. Decrypted traffic can be obtained from target's protocol stack [22] or by reverse engineering applications [23]. Central IDS, CIDS, approach was presented by Goh et al. [24]–[26]. Their solution mirrored the traffic to a CIDS, which was able to decrypt the traffic and perform deep packet inspection to the decrypted traffic. They used Shamir's secret sharing scheme and VPN. The compromised host problem is addressed. However, this solution required decryption and therefore is only suitable to limited range of network configurations. The encrypted traffic IDS solutions, which require decrypting can use the same detection approaches as traditional IDS. Therefore, the accuracy of their solutions is not the main interest here as the accuracy of the IDS is not related to encryption.

From the literature discussed so far it is shown that different types of actions and patterns can be identified from encrypted traffic without decryption. The solutions that do not require decryption are more interesting as they could use the methods used in traffic analysis attacks and encrypted traffic classification. The suitability of traffic analysis methods for detection operations in high speed networks have been addressed by Hellemons et al. [27] and Amoli et al. [28], [29].

One of the earliest publications on encrypted traffic IDS was made by Joglekar and Tate [30]. Their solution ProtoMon was based on detection of protocol misuse. Even though this approach is limited to detection of protocol violations only, it formed a basis for many of the other studies discussed in this survey.

Yamada et al. [31] proposed an approach, which only uses data size and timing information without decrypting the traffic. By comparing client's access frequency to the characteristic of normal accesses it was determined whether the access was malicious or not. They tested the method by using an actual dataset gathered at a network gateway and DARPA dataset. For DARPA dataset they added random padding for each data size to simulate the encryption. They tested three different attack classes: Scanning attacks, scripting vulnerabilities and buffer overflows. The results for the actual dataset were good with low false alarm and low false negative rates. Different types of attacks were distinguished from normal accesses. However, they were not able to detect all attacks from the DARPA dataset mainly because some of the attacks did not include a scanning phase before the intrusion. They state that this situation differs from an actual network attack scenario and therefore future work should focus on different datasets.

Foroushani, Adibnia, and Hojati [32] also used traffic analysis methods to detect intrusions without decrypting the traffic. They focused on detecting the attacks from accesses with SSH2 protocol to network public servers. The method was implemented on Snort IDS and evaluated using DARPA dataset. In scanning attacks, the requests are similar to normal requests but responses are smaller than normal. Script language attacks are similar to normal HTTP traffic when the attack is successful (small request, large response). However, when the attacker is looking for vulnerable applications, the attack evokes small responses with error messages. This pattern can be used to detect abnormal activities. Buffer overflow attacks send large requests in order to overflow the vulnerable buffer. They show that their method is able to detect intrusions with false alarm rate of about 15 % and scanning, script and buffer overflow attacks are detected with high accuracy. Numerical results for accuracy are not given. The reasoning for detecting different types of attacks is clearly stated but the results for different types of attacks are not separated in the analysis. Therefore, it is impossible to tell if the presented approach is working as intended.

Koch and Rodosek [33], [34] explored a security system for encrypted environments. Their solution was based on multiple analysis blocks, namely: Command evaluation, Strategy analysis, User identification and Policy conformity. They were able to identify limited range of commands such as ‘ls –l’ and login sequences from SSH-traffic. The analysis was based on the sizes of input packet series, size of answer packet series, divergences in packet sizes, server delays arising from system access and split answer packet series. The analysis is based on both the sender packets and the server answers.

Augustin and Balaz [10] proposed IDS architecture that combined encrypted application recognition to the anomaly detection based pattern identification in SSL traffic. This dual approach gives more accurate information for threat classification. One of the most cited result was that encryption does not hide size information completely. No numerical test results were given.

In 2012, Hellemons et al. [27] published a flow-based SSH intrusion detection system SSHCure. It was based on a three phase state machine, which monitored packets-per-flow and minimum number of flow records. The three phases were scanning, brute force and die-off phase. Every attack had to include either scanning or brute force phase. Each phase had different threshold values for monitored features. The method was evaluated with two datasets recorded at University of Twente’s campus in 2008 and 2012. They manually inspected the dataset and found 29 (in year 2008) and 101 (in year 2012) incident in the scanning phase. Their method found correctly 28 and 100 incidents respectively and had 1 false positive in both sets. No false positives were recorded. They used to their algorithm to see how many of these attacks progressed to further phases. From the 2008 dataset, 17 attacks reached brute-force phase and 16 reached die-off phase. From the 2012 dataset, 58 attacks reached brute-force phase and 25 reached die-off phase. Correctness of these later classifications was not presented.

In 2013, Barati et al. [2] proposed a data mining solution for the encrypted traffic IDS problem and used flow-based features instead of packet features. They presented a hybrid model of Genetic Algorithm and Bayesian Network classifier for finding the best subset of features. The model was tested by trying to detect brute force attacks from SSH traffic. Their model extracted 12 most efficient features from the original 42. In classification phase, with the selected features, they received average ROC area value of 0.983 and false positive rate of 0.015. The results were promising but they state that different types of attacks need to be tested with larger dataset. In 2014, Barati, Abdullah, Udzir, Behzadi, Mahmod and Mustapha [35] published an article on SSH IDS in cloud environment. The method extracted most representative features and classified them by using the Multi-Layer Perceptron model of Artificial Neural Network. It was evaluated against brute force attacks. Their method was able to classify correctly 94 % of the instances. The ROC area value was 0.978 and False Positive Rate was1.6 %.

Amoli and Hämäläinen published in 2013 [28] an article on detecting zero-days attacks and encrypted network attacks in high speed networks. High speed network requires too much resources that a deep packet inspection based IDS would be feasible. Amoli’s and Hämäläinen’s work is suitable for both normal and encrypted networks as it only uses network flows for analysis. The real-time detection model they suggest is based on two engines. The first engine is aimed to find attacks that increase network traffic (e.g. DoS and scanning). The second engine is designed to find out botnet's master in DDoS attack. Implementation and testing the model was presented later [29]. For evaluating the first engine they extracted fast network intrusions in DoS, probes and DDoS from DARPA dataset. They received 100 % Recall, 98.39 % Accuracy and False Positive Rate of 3.61 %

In 2014, Koch et al. [36] wrote a more comprehensive article on their ideas. Their solution is based on multiple modules. They aim to detect attacks from network traffic and to identify insider threat and extrusion activities. In the case of network attacks the detection is done based on a similarity measure. This method assumes that there are more normal events than malicious. Therefore, a normal connection has high correlation to the majority of connections. Malicious connections are rare and have lower correlation to the other connection. The more similar the event is to the majority of events, the more likely it is normal. If attacker tries to influence the detection system by flooding malicious traffic, the correlations of normal connections drop. However, this behavior can be detected as well. In the case of small amounts of connections, this similarity measure is not applicable. Their proposed method uses intra-session correlation, which uses segments of one connection for correlations. Extrusion- and insider detection uses command identification and attack trees to identify possible attacks. Sequence evaluator is used to analyze if the used sequence of commands is a part of known attacks. Personal typing characteristics are used to confirm the identity of the user. Then the authorization verification module verifies if the action is allowed for this user. Once all the evaluation results are accomplished the Action Selection can form automatic firewall rules when needed. The evaluation was done on a HTTPS webshop. Users and normal traffic were simulated using Tsung benchmarking tool. Brute force login attempts and SQL injections were added to the traffic. Up to 63 parallel user connections were simulated and malicious traffic varied between 1 % and 2.7 % of the connections. Network attacks were identified with accuracy of 72.05 – 74.39 % with false alarm rates of 27.80 – 25.92%. The article combines the detection results of both SQL injections and brute force attempts, therefore it is not possible to evaluate the detection performance for each attack by itself.

In 2015, Zolotukhin et al. [37] presented data mining based solution to detect DoS attacks. They implemented DBSCAN algorithm and compared it to other well-known algorithms: K-means, K-Nearest Neighbors, Support Vector Data Description (SVDD) and Self-Organizing Map. All but SVDD performed with accuracy over 99.99 %. SVDD achieved an accuracy of 99.94 %. The false alarm rate for the DBSCAN approach was lowest being 0.0697 %. This confirms that detection of DoS attack is relatively accurate even in encrypted traffic.

Table 3. Intrusion detection solutions that do not require decryption.

Article	Method	Attack types	Cons
[30]	Protocol misuse detection	Protocol misuse	Only protocol misuse detection
[31]	Data size, timing. Datasets: Darpa and live recording	Scanning, scripting language vulnerabilities, buffer overflow	Attacks must contain scanning phase
[32]	Data size, time interval. Dataset: Darpa	Scanning, script, buffer overflow	Attacks are not separated in analysis
[33]	Statistical command evaluation	Identifies commands	
[34]	Command evaluation, Strategy analysis, User identification and policy conformity. No testing.		
[36]	Similarity measurements	Brute force, SQL injection	Attacks are not separated in analysis
[10]	Application identification. No testing.	DoS	
[27]	3 state machine, Packets-per-flow and minimum number of flow records	SSH: Scanning, brute-force, exploit	Attacks must contain scanning or brute force phase
[28]	DBSCAN No testing.	DoS, DDoS, scanning, zero days, botmaster	
[2]	Choosing most effective features with Genetic Algorithm	Brute force	
[35]	Artificial Neural Network (Multi-Layer Perceptron)	Brute force	
[37]	DBSCAN	DDoS	
[29]	DBSCAN	DoS, DDoS, scanning, zero days, botmaster	

Most of the encrypted traffic IDS papers using the traffic analysis approach focus on relatively small amount of different attacks. The most frequent ones are different DoS attack scenarios and scanning attacks. Traffic analysis fares well against this type of threats but only few articles state the performance against more difficult types of attacks such as SQL injection. Another common feature is that only successful detections are reported. Articles do not evaluate detections methods across various scenarios but focus on few relatively easy use cases. In table 3 are presented the articles discussing possible solutions for encrypted traffic IDS. The solutions are based on either protocol analysis or traffic analysis and do not require decryption.

The majority of articles presented in table 3 do only limited testing on mass attack types such as scanning, brute force and DoS. Few list other types of attacks in their test sets but the results have limitations. First limitation is that attacks have to have some sort of mass attack component. Either scanning or brute force phase is required before subtler attacks can be detected. Another type of limitation is in presenting the results. The attack traffic contains subtler attacks but results are only reported for the whole attack data. This leaves the possibility that the detection rate is based on the noisier attacks alone.

4 Discussion and conclusions

Although several papers discussing encrypted traffic IDSs have been published, only few of them challenge the current detection boundaries. Even negative results would increase the valid information available. Currently it seems that attacks that distinctly change the normal traffic pattern, can be distinguished with relatively high accuracy. This is enough to detect various DoS / DDoS, brute force and scanning attacks that are based on the amount of messages.

Future research should be made systematically. Detection features and attacks in tables 1 and 2 give a basis for creating test sets. Testing should be conducted with large dataset consisting of multiple types of attacks. Thorough consideration should be used while choosing the dataset. For example, the DARPA dataset might give too promising results if both the training and testing are done only using it because the DARPA dataset has documented disadvantages (see e.g. [38], [39]). To some extent, using the same dataset for both training and testing can cause problems, such as overfitting, in all datasets.

The reporting of results should also be made systematically and the results should include negative findings when the approach is unable to detect certain types of attacks. Using clear numerical results instead of descriptions makes comparison possible. Recommended values include at least accuracy and false alarm rate. For more detailed analysis, true positive, false positive, true negative and false negative values, Receiver Operating Characteristic curve (ROC) and area under curve (AUC) should be presented. By testing attack types that at first seem hard to detect and reporting even the negative results, it is possible to realistically evaluate the limits of detection.

We acknowledge wholeheartedly that this research is far from trivial. The environment is complex and changing from scenario to other. Still we see that the detection of subtler attacks than scanning, brute force and DoS is possible. This is based on detection results on near field research on traffic analysis attacks and encrypted traffic classification. In this article, we have analyzed encrypted traffic security challenges and presented a comprehensive review of the research work on encrypted traffic IDSs. Our analysis identifies that regardless of the way encrypted traffic is analyzed, there is yet more to be done; more untapped potential and more unresolved challenges.

References

[1] R. Koch, “Towards next-generation Intrusion Detection,” in *2011 3rd International Conference on Cyber Conflict (ICCC)*, 2011, pp. 1–18.

[2] M. Barati, A. Abdullah, R. Mahmod, N. Mustapha, and N. I. Udzir, “Feature selection for IDS in encrypted traffic using genetic algorithm,” in *Proceedings of the 4th International Conference on Computing and Informatics,(ICCI’13)*, 2013, pp. 279–285.

[3] K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton, “Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail,” in *2012 IEEE Symposium on Security and Privacy (SP)*, 2012, pp. 332–346.

[4] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, “An Overview of IP Flow-Based Intrusion Detection,” *IEEE Commun. Surv. Tutor.*, vol. 12, no. 3, pp. 343–356, Third 2010.

[5] V. Engen, “Machine learning for network based intrusion detection,” Bournemouth University, 2010.

[6] J. G. Paradis and M. L. Zimmerman, *The MIT guide to science and engineering communication*. MIT Press, 2002.

[7] M. Liberatore and B. N. Levine, “Inferring the source of encrypted HTTP connections,” in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 255–263.

[8] A. Hintz, “Fingerprinting websites using traffic analysis,” in *Privacy Enhancing Technologies*, 2002, pp. 171–178.

[9] G. D. Bissias, M. Liberatore, D. Jensen, and B. N. Levine, “Privacy vulnerabilities in encrypted HTTP streams,” *Lect. Notes Comput. Sci.*, vol. 3856, p. 1, 2006.

[10] M. Augustin and A. Balaz, “Intrusion detection with early recognition of encrypted application,” in *2011 15th IEEE International Conference on Intelligent Engineering Systems (INES)*, 2011, pp. 245–247.

[11] J.-F. Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems,” in *Designing Privacy Enhancing Technologies*, H. Federrath, Ed. Springer Berlin Heidelberg, 2001, pp. 10–29.

[12] R. Alshammari, P. I. Lichodzijewski, M. Heywood, and A. N. Zincir-Heywood, “Classifying SSH Encrypted Traffic with Minimum Packet Header Features Using Genetic Programming,” in *Proceedings of the 11th Annual Conference Companion on Genetic and Evolutionary Computation Conference: Late Breaking Papers*, New York, NY, USA, 2009, pp. 2539–2546.

[13] R. Alshammari and A. N. Zincir-Heywood, “A flow based approach for SSH traffic detection,” in *IEEE International Conference on Systems, Man and Cybernetics, 2007. ISIC*, 2007, pp. 296–301.

[14] R. Alshammari and A. N. Zincir-Heywood, “Investigating Two Different Approaches for Encrypted Traffic Classification,” in *Sixth Annual Conference on Privacy, Security and Trust, 2008. PST ’08*, 2008, pp. 156–166.

[15] R. Alshammari and A. N. Zincir-Heywood, “Machine learning based encrypted traffic classification: Identifying SSH and Skype,” in *IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009*, 2009, pp. 1–8.

[16] R. Alshammari and A. N. Zincir-Heywood, “Can encrypted traffic be identified without port numbers, IP addresses and payload inspection?,” *Comput. Netw.*, vol. 55, no. 6, pp. 1326–1350, Apr. 2011.

[17] D. J. Arndt and A. N. Zincir-Heywood, “A comparison of three machine learning techniques for encrypted network traffic analysis,” in *Computational Intelligence for Security and Defense Applications (CISDA), 2011 IEEE Symposium on*, 2011, pp. 107–114.

[18] C. Bacquet, K. Gumus, D. Tizer, A. N. Zincir-Heywood, and M. I. Heywood, “A comparison of unsupervised learning techniques for encrypted traffic identification,” *J. Inf. Assur. Secur.*, vol. 5, pp. 464–472, 2010.

[19] Z. Cao, S. Cao, G. Xiong, and L. Guo, “Progress in Study of Encrypted Traffic Classification,” in *Trustworthy Computing and Services*, Y. Yuan, X. Wu, and Y. Lu, Eds. Springer Berlin Heidelberg, 2012, pp. 78–86.

[20] J. Erman, A. Mahanti, M. Arlitt, I. Cohen, and C. Williamson, “Offline/realtime traffic classification using semi-supervised learning,” *Perform. Eval.*, vol. 64, no. 9–12, pp. 1194–1213, Oct. 2007.

[21] G. Maiolini, A. Baiocchi, A. Rizzi, and C. Di Iollo, “Statistical Classification of Services Tunneled into SSH Connections by a K-means Based Learning Algorithm,” in *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, New York, NY, USA, 2010, pp. 742–746.

[22] A. A. Abimbola, J. M. Munoz, and W. J. Buchanan, “NetHost-Sensor: Investigating the capture of end-to-end encrypted intrusive data,” *Comput. Secur.*, vol. 25, no. 6, pp. 445–451, Sep. 2006.

[23] F. Kilic and C. Eckert, “iDeFEND: Intrusion Detection Framework for Encrypted Network Data,” in *Cryptology and Network Security*, M. Reiter and D. Naccache, Eds. Springer International Publishing, 2015, pp. 111–118.

[24] V. T. Goh, J. Zimmermann, and M. Looi, “Towards Intrusion Detection for Encrypted Networks,” in *International Conference on Availability, Reliability and Security, 2009. ARES ’09*, 2009, pp. 540–545.

[25] V. T. Goh, J. Zimmermann, and M. Looi, “Experimenting with an Intrusion Detection System for Encrypted Networks,” *Int. J. Bus. Intell. Data Min.*, vol. 5, no. 2, pp. 172–191, Jan. 2010.

[26] V. T. Goh, J. Zimmermann, and M. Looi, “Intrusion detection system for encrypted networks using secret-sharing schemes,” in *International Journal of Cryptology Research*, Hotel Equatorial, Melaka, Malaysia, 2010.

[27] L. Hellemons, L. Hendriks, R. Hofstede, A. Sperotto, R. Sadre, and A. Pras, “SSHCure: A Flow-Based SSH Intrusion Detection System,” in *Dependable Networks and Services*, R. Sadre, J. Novotný, P. Čeleda, M. Waldburger, and B. Stiller, Eds. Springer Berlin Heidelberg, 2012, pp. 86–97.

[28] P. V. Amoli and T. Hämäläinen, “A real time unsupervised NIDS for detecting unknown and encrypted network attacks in high speed network,” in *2013 IEEE International Workshop on Measurements and Networking Proceedings (M N)*, 2013, pp. 149–154.

[29] P. V. Amoli, T. Hämäläinen, G. David, M. Zolotukhin, and M. Mirzamohammad, “Unsupervised Network Intrusion Detection Systems for Zero-Day Fast-Spreading Attacks and Botnets,” *Int. J. Digit. Content Technol. Its Appl.*, vol. 10, no. 2, pp. 1–13, Mar. 2016.

[30] S. P. Joglekar and S. R. Tate, “ProtoMon: embedded monitors for cryptographic protocol intrusion detection and prevention,” in *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004*, 2004, vol. 1, p. 81–88 Vol.1.

[31] A. Yamada, Y. Miyake, K. Takemori, A. Studer, and A. Perrig, “Intrusion Detection for Encrypted Web Accesses,” in *21st International Conference on Advanced Information Networking and Applications Workshops, 2007, AINAW ’07*, 2007, vol. 1, pp. 569–576.

[32] V. A. Foroushani, F. Adibnia, and E. Hojati, “Intrusion detection in encrypted accesses with SSH protocol to network public servers,” in *International Conference on Computer and Communication Engineering, 2008. ICCCE 2008*, 2008, pp. 314–318.

[33] R. Koch and G. D. Rodosek, “Command Evaluation in Encrypted Remote Sessions,” in *2010 4th International Conference on Network and System Security (NSS)*, 2010, pp. 299–305.

[34] R. Koch and G. D. Rodosek, “Security system for encrypted environments (S2E2),” in *Recent Advances in Intrusion Detection*, 2010, pp. 505–507.

[35] M. Barati, A. Abdullah, N. Udzir, M. Behzadi, R. Mahmod, and N. Mustapha, “Intrusion detection system in secure shell traffic in cloud environment,” *J. Comput. Sci.*, vol. 10, no. 10, p. 2029, 2014.

[36] R. Koch, M. Golling, and G. D. Rodosek, “Behavior-based intrusion detection in encrypted environments,” *Commun. Mag. IEEE*, vol. 52, no. 7, pp. 124–131, 2014.

[37] M. Zolotukhin, T. Hämäläinen, T. Kokkonen, A. Niemelä, and J. Siltanen, “Data Mining Approach for Detection of DDoS Attacks Utilizing SSL/TLS Protocol,” in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Springer, 2015, pp. 274–285.

[38] J. McHugh, “Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory,” *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, pp. 262–294, 2000.

[39] M. V. Mahoney and P. K. Chan, “An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection,” in *Recent Advances in Intrusion Detection*, 2003, pp. 220–237.

II

CYBER THREAT LANDSCAPE IN ENERGY SECTOR

Kovanen, T., Nuojua, V., & Lehto, M., 2018

ICCWS 2018, 13th International Conference on Cyber Warfare and Security.

Reproduced with kind permission by Academic Conferences International.

Abstract

Energy, in its many forms, is vital for modern society. It is not j'ust the electricity we get from the plug but it contains the varied production methods and the means to bring it to the end-users whether they are industries, traffic or homes. If this chain is broken and energy cannot be distributed, the results are complicated. Especially, the lack of electricity tests the reserve power production capabilities in hospitals and in other critical infrastructures. Readiness plans have to be kept up to date and rehearsed regularly in order to keep them effective. This requires information of the changes in security scenarios based on new emerged threats. Energy sector is facing new opportunities as smart grid solutions provide possibilities for more efficient energy production, transmission and distribution. However, new risks arise from connectivity and automation. Bringing remote access to systems that are not designed for it security-wise, aids adversaries to reach their goals undetected. We have seen cyber risks actualizing and having an effect on our physical world. In addition to causing inconvenience in society's basic functionalities, intentional power outages also shatter the sense of security. This is why national and international research projects are formed around this topic. From Finland's perspective, interest in smart and flexible energy systems is very high. In addition, our energy production is quite distributed, and there are numerous operators on the market. Because of that, we need to consider the cyber threats in national level. There are studies and models on how to prepare for these events or even better how to prevent them. We wish to see how realistic these models are against real-world scenarios. We survey and analyze current publicly known cyber-attacks against actors in energy sector and compare the kill chain, adversaries and impacts. We also explore mitigation strategies for future scenarios based on the findings of our analysis. The result describes current energy sector cyber threat landscape. It provides information to security solution developers in business but also in national level. Results can be seen as a baseline for future trend comparisons.

Keywords: cyber security, energy, threat, critical infrastructure, smart grid

1.Introduction

Critical infrastructure is a vital part of modern society. It is comprised for example of energy sector, health care, finance and information technology. Critical infrastructure protection (CIP) aims at securing all of these. As can be seen from the example areas, they have commonalities such as immediate impact on citizens but they also hold differences such as physical infrastructures. This means the threats they face vary. Energy sector can also be included in the users of Industrial Control System (ICS) infrastructure and there is also a community focused in ICS security. However, not all ICS users are also critical infrastructure. This means that energy sector is a special example of two interesting security areas.

Energy sector consists of all the industries involved in the processes of energy production, distribution and transmission. ICSs are used for controlling these processes. Secure architecture for ICS is discussed in SANS Institute report in 2015 (Obregon, 2015). It divides the system into four zones. These zones in order are: Enterprise, Demilitarized (DMZ), Manufacturing and Cell/Area Zones. The last two form the ICS network. Internet access should be enabled only to Enterprise zone and all communication to ICS should go through DMZ which contains Remote Access servers. Manufacturing zone includes engineering workstations and plant historian. Cell/Area zone includes three levels. The highest contains Human-machine-interface (HMI) and alert systems. The middle layer consists of programmable logic controllers (PLC), remote terminal units (RTU) and distributed control systems (DCS). The bottom one consists of sensors, actuators and valves. All zones should be separated by firewalls and monitored by intrusion detection systems (IDS). Additionally, an intrusion prevention system (IPS) should be placed to monitor traffic inside Enterprise zone. Special care should be given to security information and event management system (SIEM) and log collection. These are separated from the zones by own firewall and IDS systems. Two-factor authentication is recommended.

Communication protocols in traditional ICS networks comprises of vast amounts of different protocols out of which some are proprietary ones. This is slowly shifting towards fewer standardized protocol options to enable for example vendor independence. Few of the more common protocols include IEC 60870-5-101 (International Electrotechnical Commission, serial communication), IEC 60870-5-104 (ethernet) and DNP3 (Distributed Network Protocol, ethernet) (Clarke and Reynders, 2004). Newer candidate is IEC 61850 which has more features described than just communication (Tilaro, Copy and Gonzalez-Berges, 2014). As smart grid solutions become more common, the importance of communication increases. Standards and protocols help to build a more controlled and analyzed smart grid solutions. However, the sheer volume of various standards makes it difficult to find appropriate standard. OLE (Object Linking and Embedding) for Process Control (OPC) protocol is an interface used for communication between ICS applications (Nelson, 2016). According to Stouffer et al. (2014) it should be allowed only between ICS and DMZ networks, not between the DMZ and corporate networks. Kuzlu et al. (2017) presented the most common standards and protocols related to smart grid. They state four aspects that still need more attention: interoperability, lack of awareness of the standards, technical dependencies and complexity of the system.

The consequences of an attack can be estimated by examining the effects of energy production and/or distribution malfunctions. Massive blackouts, such as in New York in August 14 - 15 in 2003, challenge the resiliency of the nation. Even though the blackout lasted only two days and was not in the middle of winter, it was estimated that mortality rate increased 28 % (90 excess deaths) and remained elevated during the remainder of August. Causes for the increase were mainly disease-related due to limited use of medical devices, slower ambulance response times and, for example, having to use stairs instead of elevator, which caused one reported heart attack (Anderson and Bell, 2012).

The rest of the paper is organized as follows. In section 2, we shortly present the concepts related to the cyber threat in energy sector. In section 3, we introduce the actual attack cases and in section 4, we discuss of the knowledge derived from those cases. Finally, section 5 presents our conclusions.

2.Perceiving the threat

Energy sector among other traditional sectors using ICSs is facing a change in security culture. Before it was adequate to ensure the physical security of systems. As cyber threats emerged, companies needed to develop methods for ICS cyber security. SANS has been surveying this development in the past years and published the results yearly. In the 2017 report (Gregory-Brown, 2017) they state that 69 % of the surveyed IT and ICS security practitioners consider the threat to ICS systems to be high or severe/critical. Special concerns arise from the (Industrial) Internet of Things and the convergence of IT and operational technology.

CIP is a studied subject that includes cyber security of electricity production, transmission and distribution. ICS related cyber security recommendations are available from e.g. SANS (Obregon, 2015) but especially power grid related security studies are rare (Jarmakiewicz et al., 2017). Smart grid security is another rising concern among industry. Increased connectivity increases cyber related risks in energy sector. Various threat models and protection plans are presented in e.g. Baig et al. (2013) and Yang et al. (2011). However, most of the studies focus on predicting vulnerabilities and only present a very limited selection of actual attacks. We see that learning from history is essential in building a holistic situational awareness picture. Therefore, we wish to add a more comprehensive study of actual events to increase common knowledge.

ICS Kill Chain was presented in 2015 by SANS institute (Assante and Lee, 2015). It was a two-stage model describing the steps of a ICS targeted campaign. The first stage of an attack is similar to other targeted attack campaigns. It contains the same steps that are used for example in Enisa's threat landscape report (Enisa, 2016) to describe the flow of an attack. These steps include reconnaissance, delivery, exploit, install, C2 and act. This stage is usable for espionage motivated attacks and as a first stage in ICS operation affecting campaigns. The second stage describes the ICS related part of the campaign. It consists of development, test, deliver, install and execute steps. Executing the attack may have separate categories: enabling, initiating and supporting.

Attribution of cyber attacks is complicated as evidence is easily forged in digital environment and the sheer volume of information might be difficult to handle. When commonly available attack methods, such as IP address spoofing, are used, the identity of attacker remains hidden. While determining the identity of the attacker there are questions to be asked on technical/tactical, operational and strategical level (Rid and Buchanan, 2015). These questions on a technical level answer the questions of what and how. For example, the used infrastructure such as command-and-control server and indicators of compromise are investigated. On operational level the questions are more related to who was behind the attack and what was the context of the incident. For example, high required resources imply to a state-(sponsored)-actor. On strategic level the question is why and how to react. Our study is mostly addressing the technical and operational questions. Strategical questions are left for future study.

3.Actualized cyber threats

The threat scenarios presented here are based on a limited amount of academic studies and white papers or reports from known sources such as security companies. These sources offer reliable information on actual cyber attacks in energy sector but there are a few limitations. We only get to see the attack analysis that are decided to be published. Therefore, situational awareness picture might lack unknown components. Also, technical details are kept to minimum or released only to paying customers. This might have effect on developing technical protection systems but it has less effect on forming a comprehensive view of the situation. While the technical details of an incident are usually widely agreed on, the interpretation of actor, motivation or significance vary depending on the analyzing organization and individuals. Usually interpretation of official sides is more conservative and gets near guessing in some forms of press material or social media.

Difficulties in source selection arise mostly from the press material. Cyber attacks against critical infrastructure offer shocking headlines and factual content may be of secondary concern. Especially interpretation part of analysis is often biased to more startling direction. Also, press does not reveal its sources and therefore the credibility can not be estimated. Often the target companies refuse to comment cyber attack allegations (Harp and Gregory-Brown, 2016) or state shortly that there was an incident and it has been dealt with. The motivation of these press statements is to assure clients and business partners of the continuity of operation and not to provide new information of the incident.

McAfee released a white paper on cyber attacks targeting the Kazakh, Taiwanese, Greek and US energy sector (McAfee, 2011). The purpose of the attacks starting from the late 2009 was to access some highly confidential information by using for example social engineering, spear phishing, vulnerabilities in Windows operating system and remote administration tools. First, they compromised the extranet web servers by using SQL (Structured Query Language) injection. Through the compromised web server, they got access to internal desktops and servers. After that, they launched spear phishing attacks on the laptops using VPN (Virtual Private Network) connection and used password stealing tools in order to get an additional access. In addition, they installed remote administration tools and the malware itself. Finally, they found out which computers belonged to the executives and captured their emails and files. According to McAfee, the group behind the attacks, "Night Dragon", has been active at least since 2009, even earlier. Based on the hacking tools and locations used in the attack, they strongly believe that the attackers were situated in China.

Symantec discovered the Shamoon, or W32.Disttrack, malware targeting the Saudi Arabian energy sector in August 2012 (Symantec Security Response, 2012a). The malware has three components: Dropper, Wiper and Reporter. The main component, Dropper, is responsible for infecting the target and for dropping the other modules. The Wiper module is responsible for destructing the files and for overwriting the master boot record (MBR) of the infected computer. The Reporter module is responsible for reporting to the attacker. Once Shamoon gets inside the network, it utilizes the network shares in order to spread into every computer in the LAN (Symantec Security Response, 2012b). Shamoon made a comeback in November 2016. The most visible difference between the 2012 and 2016 attacks was the differing image overwritten in the MBR (Symantec Security Response, 2016). According to FireEye, the group behind Shamoon attacks is an Iranian group called "Cutting Sword of Justice" (FireEye, 2016b). Paganini

(2012) based his assessment of the Iranian origin on the dispute Iran has had with the target of the attacks, Saudi Aramco, Saudi Arabian oil company.

Symantec published a white paper on a pure cyber espionage campaign against energy sector in July 2014 (Symantec Security Response, 2014). In order to get into targeted organizations, the attackers utilized spear phishing emails with malicious PDFs attached, and watering hole attacks. After that, they deployed the Lightsout (later known as Hello) exploit kit that utilized browser and Java exploits to deliver either one of the main malware tools: Trojan.Karagany or Backdoor.Oldrea. The choice was made based on the available information. Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT (Remote Access Tool), was customized specifically for this attack. It utilized the OPC protocol in order to map out the ICS devices (Nelson, 2016). The purpose was to enable the attacker to extract system information and install other malwares to the compromised computer. Trojan.Karagany, in turn, was used mainly for reconnaissance but also for data exfiltration and for downloading and installing additional files. Symantec named the group behind the attack as "Dragonfly", while some call it "Energetic Bear". The group has been active at least since 2011 but targeting the US and European energy sector since 2013. According to Symantec, the attacks seem to be state-sponsored because of their sophistication and the group's high technical capabilities. In addition, they inferred that the attackers might be situated in Eastern Europe based on the analysis of malware timestamps. The second campaign, "Dragonfly 2.0", started at the end of 2015 and targeted at least US, Swiss and Turkish energy sector (Symantec Security Response, 2017). It had quite the same features as its predecessor but for example used a new version of Trojan.Karagany: Trojan.Karagany.B. Related to the second attack wave, Symantec revealed that there were both Russian and French code in the malware but stated that those might have been put there to mislead.

Iranian cyber activities in critical infrastructure systems were studied by security company called Cylance in 2014 (Cylance, 2014). Their report on Operation Cleaver date activities starting from 2012 until the publication of the paper. Targets vary from aerospace industry to education, and attacks against energy companies have been found in Canada and United States. Attacks against oil and gas companies are reported in Canada, France, Kuwait, Mexico, Qatar, Saudi Arabia and Turkey. Main goal was to exfiltrate information of critical infrastructure systems that could enable further attacks. Reuters (Finkle, 2014) was able to name a few of the targets. U.S. energy company Calpine Corp, state-controlled oil companies Saudi Aramco and Petroleos Mexicanos were among them. Attribution of Operation Cleaver is given to Iranian actors due to naming conventions, infrastructure registered in Iran, tools set to warn if IP addresses trace back to Iran. Cylance also believes this campaign was sponsored by Iran based on the significance of used infrastructure.

The attack against three distribution level energy companies in Ukraine in December 2015 caused a blackout that lasted for hours and recovery process took months. It was analyzed in E-ISACS defense use case study (Lee, Assante and Conway, 2016a). According to them the attack affected to seven 110 kV and 23 35 kV substations and left 225 000 customers without electricity. The attack campaign had lasted at least 6 months before the blackout, and reconnaissance information was presumably gathered from open sources, such as ICS vendor brochures. The initial intrusion was made using a modified version of BlackEnergy 3 malware, which was used as a backdoor to administrative and IT networks of the energy companies. The malware was delivered through spear phishing emails containing an Office document that, after user enabling macros, installed the malware. Through the backdoor attacker secured persistence, charted company systems and collected credentials which in turn allowed the use of corporate VPN and finally granted the access from the business network to ICS network. The final attack was done using legitimate commands that opened substation breakers and thus, prevented electricity distribution. The supporting attacks ensured that the restoration had to be done manually. These supporting actions included installing and executing KillDisk malware on operator workstations. KillDisk rendered operation workstations unusable and removed log information. Also, malicious firmware was installed on serial-to-ethernet gateway at the substations preventing remote communication. This was to keep operators from restoring breakers remotely if operator workstations were recovered. DoS (Denial of Service) attack was done telephonically to call centers preventing customers to reach energy companies. This frustrated customers but it also prevented companies to evaluate the scale of the blackout and to coordinate restoration attempts.

Ukraine 2015 attack is attributed to a group called Sandworm (FireEye, 2016a). It is a cyber attacker group most famous for its energy sector related sabotage campaign but is has had also espionage activities. The first sightings of this group are from the summer of 2014 when it was connected to Windows OLE Remote Code Execution Vulnerability attacks (MITRE, 2014) that were espionage attacks against various governmental target within Europe and NATO (TrendLabs Security Intelligence Blog, 2014). Signature malware of Sandworm team is the BlackEnergy malware which has advanced to its third generation (FireEye, 2016a). However, not all attacks done using BlackEnergy are done by Sandworm as the earlier generations are available from the net (F-Secure Labs, 2014). At first BlackEnergy was used to create botnets for DoS attacks and it was used by criminal groups as it was sold as a crimeware. Malware was then developed to enable more attack types such as spamming and espionage. It was used in Estonia related to the relocation of Bronze Soldier of Tallinn in 2007 (Shamir, 2016) and during in the Russo-Georgian confrontation in 2008 (F-Secure Labs, 2014). From 2014 onwards, the use of BlackEnergy malware has moved on to Ukrainian targets, most notoriously, it was used in the blackout in 2015 (Lee, Assante and Conway, 2016a). Sandworm team is also using wiper malwares as a part of their campaigns. They used KillDisk during Ukraine 2015 incident (Lee, Assante and Conway, 2016a). Ukraine 2015 attackers are also related to NotPetya campaign in 2017 (Cherepanov, 2017a; Cherepanov, 2016). NotPetya targeted Ukrainian targets and it was first classified as a ransomware but later reclassified as a wiper which was cloaked as a ransomware (Mathews, 2017). Also, the link to Bad Rabbit ransomware/wiper attacks, that hit for example metro in Kiev, is suspected (M.LéveiNé, 2017). Sandworm team is said to be related to groups named: TeleBots, Temp.noble, Quedagh and Electrum (Cimpanu, 2017; Cherepanov, 2016), but we were unable to verify the origin of this statement. Ukranian officials have directly attributed Russia (Da Silva, 2017), and FireEye (2016a) found documents from BlackEnergy 3's command and control server that suggest the operators are Russian speakers. Also, the targets align with the interest of the Russian state. However, attributing a state directly, is not that simple, since these markers could apply to state sponsored actors, hacktivists and actors wishing to appear as the state of

Russia. Using proxy actors to hide the real adversary complicates attribution in cyber environment (Geary, 2017).

Even though, the Ukraine 2016 attack has gained less attention it was more sophisticated than the attack in 2015. It only caused a short black out but experts believe it was only to demonstrate some of its capabilities and not utilizing its full potential. Cyber security experts have investigated the malware and validated its potential (Dragos, 2017; Cherepanov, 2017b). The attack and malware used lessons learned from multiple earlier campaigns and incidents. Idea to use malware to disrupt ICS was copied from Stuxnet, using OPC protocol to map out targets came from Havex and from Blackenergy 2 came the usage of HMI to communicate with Internet connected locations. As in the attack in 2015, native systems were used against themselves. The novelty of this attack was the combined capability and the modular structure of the malware. It was not designed to be used solely in Ukraine and new protocols and attacks could be implemented to it with relative ease. The malware used was named as CrashOverride by Dragos (Dragos, 2017) and as Industroyer by Eset (Cherepanov, 2017b). It was a used as a main backdoor and was capable of installing secondary backdoor and to execute a launcher. The launcher controlled a modular structure of elements which were able to use different ICS protocols suitable to the target. The communication to ICS differed from the 2015 attack because this time the malware itself was used to communicate to ICS and not the native communication methods of the target organization. The protocols were arranged in a modular fashion enabling extensions for later use. The launcher also controlled a data wiper element which can be used to delay restoration attempts and to hide evidence. Ukraine 2016 attack is attributed to a group called Electrum (Dragos, 2017). According to Dragos, Electrum has direct ties to the Sandworm group, which performed the earlier attack in 2015.

In 2013, Iranian attackers were accused of infiltrating a dam in New York and stealing information from energy company Calpine Corp. In 2016 these incidents were critically examined in SANS ICS Defense Use Case 4 (Lee, Assante and Conway, 2016b). The small dam is not built for energy production purposes but to control water levels. The system was directly connected to Internet and there was no need for the attacker to go past business network nor DMZ. The automation system of controlling the operation of the gate was not active and therefore it is not possible to evaluate the adversary's capabilities regarding the control system because it could not have been operated remotely. Calpine is an interesting target because it has 80 power plants in operation or under construction and its estimated power production capability is 26 000 megawatts of electricity (Calpine.com., 2017). Calpine's data theft was made through 3rd party contractor and no Calpine network, neither business nor ICS, was breached. However, information such as password or network structure are valuable for an adversary planning further attacks. Attributions of these two attacks were not confirmed to be of Iranian origin even though Iranian hacktivist claimed responsibility for the dam attacks and the incidents were connected to the Operation Cleaver (Lee, Assante and Conway, 2016b). These two cases emphasize that even the smaller structures are targets and their architecture should be planned carefully. Lesson from Calpine case is that ICS related data is possible to get without targeting the actual ICS or the operating organization. This makes subcontractors and other 3rd party companies target for cyber attacks.

In 2017 US officials alerted power companies of a series of breaches. One of the targets was Wolf Creek Nuclear facility in Kansas which raised numerous headlines that a nuclear facility was hacked (see e.g. Greenberg, 2017; Perlroth, 2017; Riley, Dlouhy and Gruley, 2017). Analysis of used tools revealed that credentials of senior engineer had been stolen. However, the ICS environment stayed intact and only the business network was under an attack and no operational disturbances were detected. It was speculated that the attack did not aim ICS systems but tried to install backdoors for later purposes. Attribution for this attack could not be confirmed but Russian origin is suggested based on comments of three anonymous sources (Riley, Dlouhy and Gruley, 2017).

In August 2017 Irish Independent reported that Irish electricity transmission system operator EirGrid was a target of a man-in-the-middle attack (McMahon, 2017). The attack first breached Vodafone's Direct Internet Access (DIA) service which was providing Internet access to EirGrid's interconnector site in Wales. Attackers were able to create a Generic Router Encapsulation (GRE) tunnel into the router used by Eirgrid. All traffic through DIA router were intercepted by the attacker, and Vodafone has no estimate of how much data was then transmitted through GRE tunnel. It was discovered that System Operator for Northern Ireland (SONI), owned by EirGrid, had their data intercepted too. Vodafone and National Cyber Security Centre attribute this attack to state sponsored actor but do not elaborate that estimation further.

On top of targeted cyber campaigns actors in energy sector are faced with more conventional types of cyber attacks. Typically, these are not analyzed by security companies nor largely reported. Malware infections can spread to company's laptops or even network even without specifically targeting them. Vermont utility was an example of situation where worker's laptop generated Internet traffic, that caused an alarm. The laptop was not connected to electric grid but headlines were raised (Eilperin and Entous, 2016). Also, ransomware campaigns have reached energy sector organizations, for example Israel Electric Authority (Trendmicro.com, 2016) and Lansing Board of Water and Light (Lacy and Reed, 2016). This type of threat is mostly affecting the business/office network as the delivery method is often phishing email. Ransomware is easy to detect and the attacks have not escalated to ICS networks. However, ransomware can spread to production environment as seen in healthcare sector (DW.COM, 2016).

Some information on cyber threats concerning energy sector can be deduced from larger reports. Separate cases are not analyzed but information on the scale of the threat, geolocation and adversary's motivations can be gathered.

The cyber breach response experts of FireEye, known as Mandiant, have carried out a deeper analysis on a specific Chinese APT (Advanced Persistent Threat) group called APT1 (Mandiant, 2013). Between 2006 and 2013, the cyber espionage campaign of APT1 targeted towards 141 companies in 20 different industries, located mostly in the English-speaking countries. Eight of these attacks were made against the energy sector. The purpose of the attacks was steeling valuable intellectual property. Mandiant states the claims of Chinese origin based not only on many technical observations, such as IP addresses and domain names referring to China, but also on the target industries that were identified as strategic to China's growth.

Although the most media attention has been given to the incidents in Europe and US, the situation awareness picture is far from complete. In a report of cyber threats in Southeast Asia published by FireEye states that 7 % of detected targeted attacks in the region were made against energy industry actors, and the main motivator was to obtain data of competitive value (FireEye Threat Intelligence, 2015). For example, they have observed malware deployment against a major electric grid operator. There are no more details available on this specific case but this example emphasizes that there are cases beyond public knowledge and their geolocations vary globally.

4.Lessons learned

Two major cyber attack types can be categorized, namely non-targeted and targeted attacks. Non-targeted attacks can be seen as cyber attacks that target also other sectors than energy and sometimes these attacks reach energy sector actors. These attacks include for example ransomware campaigns and non-targeted malware infections. Targeted attacks are focused on a specific target and attack campaign requires resources, such as skill and time. This type of threat is often referred as APT.

Non-targeted attacks vary from port scanning activities to ransomware and other malware infections. The quality of information published of these events vary. The companies involved often do not wish their brand to be associated with cyber risks and decline inquiries. Cyber security companies, on the other hand, publish white papers only from larger scale events and it is difficult to parse out information concerning energy sector. This leaves us media reports which often do not state their sources and unfortunately do not often discuss of the technical details. Even though non-targeted attacks are not aiming a specific operation the disturbance they cause can be as fatal as in targeted attacks. It is likely that non-targeted threats are more common than targeted attacks but underreported. This threat type is best eliminated by good cyber security practices, such as increasing knowledge of personnel about phishing emails and segmenting networks to prevent spreading.

Targeted attacks seen so far have focused on espionage or sabotage without destroying any infrastructure. Advancements in attack techniques show that attacks are evolving and reaching the finesse seen in attacks focusing traditional IT networks. Traditional security measures are not enough to counter these attacks as the adversary has time and skills to bypass them. Having strong and diverse defense in action, makes these attacks much more time consuming and increase the probability of detection before the adversary's goal is reached. For example, the security measures suggested in SANS report (Obregon, 2015), such as using two factor authentication in ICS network, would have prevented the use of password pilfering as an attack vector. Most of the targeted attacks are espionage driven and do not target ICS systems directly. However, the information and knowledge obtained through espionage can shorten the attack cycle in future. This means less chances for the defenders to detect the ongoing operation and to prevent it. Another cause for espionage is to gain competitive edge in business. Sabotage motivation has emerged in Ukraine and it is the scenario that raises most concerns. Because the energy infrastructure itself has not been harmed, it has been possible to restore operations within reasonable time. If the blackout occurs during another crisis event the consequences of even a shorter blackout are more dire. If the attack destroys the target infrastructure, as seen in Stuxnet attack (Brunner et al., 2010), the restoration can be far more complex.

The entry-point of most of the attacks resides in business network which has connection to Internet. Therefore, it is good that most of the large-scale energy structures are isolated from the Internet and require access to the business network before accessing ICS. However, it is not known how many smaller structures are directly connected to Internet because of unawareness or neglect. Usually business network has basic security measures but they can be evaded. Spear phishing attacks are common and an untrained employee can endanger the organization. If the attack gets to ICS environment, it needs to be detected during the reconnaissance phase to prevent it from escalating to full attack. The steps of ICS Kill Chain combined with the secure ICS architecture, can be used as a framework to identify promising points of detection.

Careful planning of detection and prevention methods is a must but some attacks will get through also in the future. In this situation, recovery and restoring operations are vital for both the companies and for society. In Ukraine 2015 incident the possibility to restore substations operations manually allowed the restoration of power even though remote connection was lost. In the ascent of digitalization, it is beneficial to evaluate if some controls should have a manual backup.

On-going events gain publicity rapidly but the accuracy of information varies. Common misconception is that if a part of company's network is breached the ICS operation is compromised. Open communication and educating the public could decrease the number of misleading headlines in the press. Sharing correct information would also enable fact-based discussion of the countermeasures and legislation needed to prevent large scale events.

5.Conclusions

It is evident that the energy sector, as a critical component of modern society, is a lucrative target for malicious activities. While most of the attacks are focused on gathering information, it is advisable to prepare for sabotage. Especially, preventing destruction of physical equipment is crucial. Good security practices throughout organization, including ICS environment, increase the probability to detect and to prevent an attack. In case detection and prevention fail, recovery will be to only option. Recovery from a cyber attack of various types should be planned and practiced. Also, planning press communication should not be forgotten. Correct information form the base for designing these actions. However, the cyber threat landscape in energy sector is ever changing and needs continuous monitoring. To maintain situation awareness, international communication between companies, public organizations and researchers is needed.

Future work consists of actions on a broad spectrum and therefore one actor is not enough. Joint effort is needed. Maintaining situational awareness of cyber threat landscape in energy sector needs continuous updates. Research and innovations are needed for technical protection solutions but this does not remove the human aspect out of the security equation. Communication, education, research and professional networks are assets worth developing. Another rising concern comes from the emerging of smart grid technologies which adds more digital channels affecting the energy sector operations and thorough consideration should be given to the security aspects of these solutions. This becomes more and more essential as customers start to connect energy producing or metering devices to the power grid. This increases the complexity of energy grid systems and enables more connection points for malicious devices. On the positive side, energy sector's position as a critical infrastructure actor is nothing new. This means that the mindset of securing operations in atypical situations is familiar and practiced in everyday operations. This mindset just needs to be broadened to include advanced cyber related disruptions.

References

Anderson, G. B., and Bell, M. L. (2012). Lights out: impact of the August 2003 power outage on mortality in New York, NY. Epidemiology (Cambridge, Mass.), 23(2), 189.

Assante, M. and Lee, R. (2015). The Industrial Control System Cyber Kill Chain. SANS Institute InfoSec Reading Room.

Baig, Z., and Amoudi, A. (2013). An analysis of smart grid attacks and countermeasures. Journal of Communications, 8(8), 473-479.

Brunner, M., Hofiger, H., Krauss, C., Roblee, C., Schoo, P. and Todt, S. (2010). Infiltrating critical infrastructures with next-generation attacks, W32.Stuxnet as a showcase threat. Fraunhofer Research Institute AISEC, 12/2010.

Calpine.com. (2017). Calpine. [online] Available at: http://www.calpine.com/ [Accessed 2 Nov. 2017].

Cherepanov, A. (2016). The rise of TeleBots: Analyzing disruptive KillDisk attacks. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/ [Accessed 8 Nov. 2017].

Cherepanov, A. (2017a). TeleBots are back: supply-chain attacks against Ukraine. [online] WeLiveSecurity. Available at: https://www.welivesecuritv.com/2017/06/30/telebots-back-supplv-chain-attacks-against-ukraine/ [Accessed 2 Nov. 2017].

Cherepanov, A. (2017b). WIN32/INDUSTROYER, A new threat for industrial control systems. ESET.

Cimpanu, C. (2017). Security Firms Say Bad Rabbit Attack Carried Out by NotPetya Group. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/security-firms-say-bad-rabbit-attack-carried-out-by-notpetya-group/ [Accessed 2 Nov. 2017].

Clarke, G. and Reynders, D. (2004). Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems. Newnes.

Cylance. (2014). Operation Cleaver. Report.

Da Silva, C. (2017). Russia was behind global cyber attack, Ukraine says. [online] The Independent. Available at: http://www.independent.co.uk/news/world/europe/russia-cyber-attack-ukraine-petya-telebots-blackenergy-sbu-cadbury-a7819501.html [Accessed 9 Nov. 2017].

Dragos. (2017). CRASHOVERRIDE, Analysis of the Threat to Electric Grid Operations. Version 2.20170613. Report.

DW.COM. (2016). Hackers hold German hospital data hostage. [online] Available at: http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030 [Accessed 2 Nov. 2017].

Eilperin, J. and Entous, A. (2016). Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say. [online] Washington Post. Available at: https://www.washingtonpost.com/world/national-securitv/russian-hackers-penetrated-us-electricitv-grid-through-a-utilitv-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f story.html?utm term=.367fce52a417 [Accessed 2 Nov. 2017].

Enisa. (2016). ENISA Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends, final version 1.0.

F-Secure Labs. (2014). BlackEnergy & Quedagh: The convergence of crimeware and APT attacks. F-Secure Labs whitepaper.

Finkle, J. (2014). Iran hackers targeted airlines, energy firms: report. [online] Reuters. Available at: http://www.reuters.com/article/us-cybersecurity-iran/iran-hackers-targeted-airlines-energy-firms-report-idUSKCN0JG18I20141202 [Accessed 31 Oct. 2017].

FireEye. (2016a). Cyber attacks on the Ukrainian grid: what you should know. FireEye industry intelligence report.

FireEye. (2016b). FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region. [online] Available at: https://www.fireeye.com/blog/threat-research/2016/11/fireeye respondsto.html [Accessed 25 Oct. 2017].

FireEye Threat Intelligence. (2015). Southeast Asia: An Evolving Cyber Threat Landscape. Special report.

Geary, S. (2017). The Cyber-Intelligence Nexus: Russia's Use of Proxies. [online] The Cipher Brief. Available at: https://www.thecipherbrief.com/the-cyber-intelligence-nexus-russias-use-of-proxies-2 [Accessed 8 Nov. 2017].

Gregory-Brown, B. (2017). Securing Industrial Control Systems-2017. SANS Institute InfoSec Reading Room.

Greenberg, A. (2017). Hack Brief: Hackers Targeted a US Nuclear Plant (But Don't Panic Yet). [online] WIRED. Available at https://www.wired.com/story/hack-brief-us-nuclear-power-breach/ [Accessed 2 Nov. 2017].

Harp, D., Gregory-Brown, B. (2016). SANS 2016 State of ICS Security Survey. SANS Institute InfoSec Reading Room.

Jarmakiewicz, J., Parobczak, K., and Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. International Journal of Critical Infrastructure Protection, 18, 20-33.

Kuzlu, M., Pipattanasompom, M., and Rahman, S. (2017). A comprehensive review of smart grid related standards and protocols. In Smart Grid and Cities Congress and Fair (ICSG), 20175th International Istanbul (pp. 12-16). IEEE.

Lacy, E. and Reed S. (2016). BWL cyberattack bills reach nearly $2M. [online] Lansing State Journal. Available at: http://www.lansingstate¡ournal.com/storv/news/local/2016/09/22/bwl-ransomware-attack-costlv-details-emerging/90826176/ [Accessed 2 Nov. 2017].

Lee, R., Assante, M. and Conway, T. (2016a). Analysis of the cyber attack on the Ukrainian power grid, Defence Use Case. EISAC.

Lee, R., Assante, M. and Conway, T. (2016b). Analysis of the recent reports of attacks on US infrastructure by Iranian Actors. SANS ICS 2016 Defense Use Case 4.

M.Léveillé, M-E. (2017). Bad Rabbit: Not-Petya is back with improved ransomware. [online] WeLiveSecurity. Available at: https://www.welivesecuritv.com/2017/10/24/bad-rabbit-not-petva-back/ [Accessed 2 Nov. 2017].

Mandiant. (2013). APT1 - Exposing One of China's Cyber Espionage Units. Report.

Mathews, L. (2017). The NotPetya Ransomware May Actually Be A Devastating Cyberweapon. [online] Forbes.com. Available at: https://www.forbes.com/sites/leemathews/2017/06/30/the-notpetva-ransomware-mav-actuallv-be-adevastating-cyberweapon/#3a16b88e39e8 [Accessed 2 Nov. 2017].

McAfee (2011). Global Energy Cyberattacks: "Night Dragon". McAfee Foundstone Professional Services and McAfee Labs, White Paper.

McMahon, C. (2017). Exclusive: EirGrid targeted by 'state sponsored' hackers leaving networks exposed to 'devious attack'. [online] Independent.ie. Available at: https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-bvstate-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html [Accessed 31 Oct. 2017].

MITRE (2014). CVE-2014-4114. [online] Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4114 [Accessed 31 Oct. 2017]

Nelson, N. (2016). The Impact of Dragonfly Malware on Industrial Control Systems. SANS Institute InfoSec Reading Room.

Obregon, L. (2015). Secure Architecture for Industrial Control Systems. SANS Institute InfoSec Reading Room.

Paganini, P. (2012). Iran suspected for the attack on the Saudi Aramco. [online] Security Affairs. Available at: http://securitvaffairs.co/wordpress/8300/malware/iran-suspected-for-the-attack-on-the-saudi-aramco.html [Accessed 8 Nov. 2017].

Perlroth, N. (2017). Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say. [online] Nvtimes.com. Available at: https://www.nvtimes.com/2017/07/06/technologv/nuclear-plant-hack-report.html [Accessed 2 Nov. 2017].

Rid, T., and Buchanan, B. (2015). Attributing cvber attacks. Journal of Strategic Studies, 38(1-2), 4-37.

Rilev, M., Dlouhv, J. and Grulev, B. (2017). Russians Are Suspects in Nuclear Site Hackings, Sources Say. [online] Bloomberg.com. Available at: https://www.bloomberg.com/news/articles/2017-07-07/russians-are-said-to-besuspects-in-hacks-involving-nuclear-site [Accessed 2 Nov. 2017].

Shamir, U. (2016). Analyzing a New Variant of BlackEnergy 3, Likely Insider-Based Execution. SentinelOne. Whitepaper.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M. and Hahn, A. (2014). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82. Revision 2 Initial Public Draft.

Svmantec Securitv Response. (2012a). The Shamoon Attacks. [online] Available at: https://www.svmantec.com/connect/blogs/shamoon-attacks [Accessed 25 Oct. 2017].

Svmantec Securitv Response. (2012b). The Shamoon Attacks Continue. [online] Available at: https://www.svmantec.com/connect/blogs/shamoon-attacks-continue [Accessed 25 Oct. 2017].

Svmantec Securitv Response. (2014). Dragonfly: Cyberespionage Attacks Against Energy Suppliers. Version 1.21.

Svmantec Securitv Response. (2016). Shamoon: Back from the dead and destructive as ever. [online] Available at: https://www.svmantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever [Accessed 25 Oct. 2017].

Svmantec Securitv Response. (2017). Dragonfly: Western energy sector targeted by sophisticated attack group. [online] Available at: https://www.svmantec.com/connect/blogs/dragonflv-western-energv-sector-targeted-sophisticatedattack-group [Accessed 26 Oct. 2017].

Tilaro, F., Copv, B. and Gonzalez-Berges, M. (2014). IEC-61850 INDUSTRIAL COMMUNICATION STANDARDS UNDER TEST. Proceedings of the 14th International Conference on Accelerator & Large Experimental Physics Control Systems [also] ICALEPCS2013, San Francisco, California, October 2013. Geneva: JACoW.

TrendLabs Securitv Intelligence Blog. (2014). MS Zero-Day Used in Attacks Against European Sectors, Industries. [online] Available at: http://blog.trendmicro.com/trendlabs-securitv-intelligence/ms-zero-dav-used-in-attacks-againsteuropean-sectors-industries/ [Accessed 2 Nov. 2017].

Trendmicro.com. (2016). Israel's Electric Authority "Hack" Caused by Ransomware. [online] Available at: https://www.trendmicro.com/vinfo/us/securitv/news/cvber-attacks/israels-electric-authoritv-hack-caused-bvransomware [Accessed 2 Nov. 2017].

Yang, Y., Littler, T., Sezer, S., McLaughlin, K., and Wang, H. (2011). Impact of cvber-securitv issues on smart grid. In Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on (pp. 1-7). IEEE.

III

HONEYPOT UTILIZATION FOR NETWORK INTRUSION DETECTION

by

Kemppainen S., & Kovanen, T. 2018

Cyber Security: Power and Technology, Springer International Publishing

DOI: 10.1007/978-3-319-75307-2_15

Request a copy from the author.

IV

BASIC ELEMENTS OF CYBER SECURITY FOR AN AUTOMATED REMOTE PILOTING FAIRWAY SYSTEM

by

Pöyhönen, J., Kovanen, T., & Lehto, M., 2021

ICCWS 2021 16th International Conference on Cyber Warfare and Security.

DOI: 10.34190/IWS.21.021

Request a copy from the author.

V

EPILOTAGE SYSTEM OF SYSTEMS' CYBER THREAT IMPACT EVALUATION

by

Kovanen, T., Pöyhönen, J., & Lehto, M., 2021

ICCWS 2021, 16th International Conference on Cyber Warfare and Security.

DOI: 10.34190/IWS.21.033

Request a copy from the author.

VI

CYBER SECURITY ANALYSIS FOR SHIPS IN REMOTE PILOTAGE ENVIRONMENT

by

Hummelholm, A., Pöyhönen, J., Kovanen, T., & Lehto, M., 2021

ECCWS 2021 20th European Conference on Cyber Warfare and Security.

DOI: 10.34190/EWS.21.025

Request a copy from the author.

VII

CYBER-THREAT ANALYSIS IN THE REMOTE PILOTAGE SYSTEM

by

Kovanen, T., Pöyhönen, J., & Lehto, M., 2021

ECCWS 2021 20th European Conference on Cyber Warfare and Security.

DOI: 10.347190/EWS.21.067

Request a copy from the author.