JYX

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Pöyhönen, Jouni; Lehto, Martti

Title: Assessment of Cybersecurity Risks: Maritime Automated Piloting Process

Year: 2022

Version: Published version

Copyright: © 2022 International Conference on Cyber Warfare and Security

Rights: CC BY-NC-ND 4.0

Rights url: https://creativecommons.org/licenses/by-nc-nd/4.0/

Please cite the original version:

Pöyhönen, J., & Lehto, M. (2022). Assessment of Cybersecurity Risks: Maritime Automated Piloting Process. In R. P. Griffin, U. Tatarand, & B. Yankson (Eds.), ICCWS 2022 : Proceedings of the 17th International Conference on Cyber Warfare and Security (17, pp. 262-271). Academic Conferences International Ltd. The proceedings of the 17th international conference on cyber warfare and security. https://doi.org/10.34190/iccws.17.1.18

Assessment of Cybersecurity Risks: Maritime Automated Piloting Process

Jouni Pöyhönen and Martti Lehto
University of Jyväskylä, Finland
jouni.a.poyhonen@jyu.fi
martti.j.lehto@jyu.fi

Abstract: A modern society is a combination of several critical infrastructures, of which international and national maritime transportation systems are essential parts. Digitalization makes it possible to increase levels of autonomy in maritime systems. It also means fully existing cyberenvironments in maritime processes. In cyberenvironments, it is crucial there is trustable information communication between system elements of the process, alongside the usability, reliability, and integrity of systems data in the operating environment. In order to develop maritime autonomy in Finland the Sea4Value / Fairway (S4VF) research program has been developed. At the first stage of the program, the main goal is to create automated fairway piloting feature in the near future. An automated remote piloting process, "ePilotage," will be a complex system of systems entity. This paper provides a research approach to investigating the cybersecurity risks at the system levels of process. It emphasizes the importation of comprehensive risk assessment to increase the cybersecurity of fairway operations. The findings of the study are located in cybersecurity risks in critical information flows between the main system blocks of the fairway process. The research question is "How can the cybersecurity risks of automated remote fairway operations be evaluated?" The main findings are related to the probabilities of the risks in all levels of process stakeholders' responsibilities. Risk assessment methodology, that has been described, is based on attack probabilities against probabilities to defend actions of adversarial in use of communication technologies. Risks assessment factors have been identified and the risk assessment tool have been proposed.

Keywords: maritime digitalization, automated piloting, cybersecurity, risks assessment, probability

1. Introduction

A modern society is a combination of several critical infrastructures, of which international and national maritime transportation systems are essential parts. Digitalization and information and communication technologies (ITC) make it possible to increase levels of autonomy in maritime systems: "ICTs are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures form a vital part of the European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures" (EU Commission, 2009). This also means fully existing cyberenvironments in maritime processes. Crucial elements in the cyberenvironment include trustable information networks and the usability, reliability, and integrity of systems data in the operating environment.

In order to develop maritime autonomy in the first stage in Finland, the Sea4Value / Fairway (S4VF) research program has been launched to create automated remote pilotage fairway features (ePilotage) in the near future: "As defined in the ePilotage Act, pilotage refers to activities related to the navigation of vessels in which the pilot acts as an advisor to the master of the vessel and as an expert on the local waters and their navigation. The purpose of pilotage is to enhance the safety of vessel traffic and prevent environmental damage generated by vessel traffic" (Finnpilot Pilotage Ltd, 2020).

The ePilotage environment of the S4FV is an example of a system of systems (SoS) in which an increased number of digital solutions are entering new environments where traditional engineering solutions are still in use. This development introduces an increased risk of a malicious cyberadversary taking deliberate actions against the system, which is why the threat analyses should be done according to the principles within the system-of-systems threat model (Bodeu & McCollum, 2018).

At the strategic level of SoS thinking, we present a description of the situation with non-technical terminology. This includes different types of adversaries based on their motivational factors: cybervandalism, cybercrime, cyberespionage, cyberterrorism, cybersabotage, and cyberwarfare. In the case of cybervandalism, the arrival of a controversial vessel in a fairway might trigger actions. The controversy might be with the cargo, the vessel's operations, or the vessel's owner. For cybercrime, valuable cargo is more tempting, with financial gain as the motivation. Cyberespionage can include business or political espionage. Political factors may arise from national or international issues. On the national side, hacktivism supporting strikes in harbors could be one scenario. In the worst case, international tensions in the region could escalate to military cyberoperations against vessel traffic (Kovanen, Pöyhönen & Lehto, 2021b).

On the operational level, we have a description of the situation with business continuity, including information on the attacker's capabilities to attack ICT and industrial control systems (ICS; Kovanen, Pöyhönen & Lehto, 2021a).

On the tactical level, we have more technical information on the threat actor's tactics, techniques, and procedures. On this level, the follow-up operations may include constant threat assessments about how the changes in an area can affect the strategic and operational levels. Threat analyses in this scope should include both user and technical views of the process. The threat probability tree model has been used for ship' cybersecurity assessment and to maintain situation awareness as an example of systems threat analyses and the risk assessment method (Hummelholm, Pöyhönen, Kovanen & Lehto, 2021).

In the ePilotage process, trustable information networks and the usability, reliability, and integrity of systems data in the fairway operating environment mainly depend on reliable information flows at the SoS levels. The cybersecurity research question related to risk assessment in this project is as follows: How can the cybersecurity risks of information flows in automated remote piloting fairway operations be evaluated?

This paper presents a research approach for cybersecurity risk assessment at the system level in the remote ePilotage process through the use of probability estimation principles. The findings of the study are situated in cybersecurity risks in critical information flows between the main system blocks of automated remote pilotage fairway and the main findings are related to the probabilities of the risks in all levels of stakeholders' responsibilities.

The paper is organized as follows: section 2 introduces automated remote pilotage fairway features, section 3 presents the basic elements of the research subject, section 4 describes a risk assessment approach done by us, section 5 discusses stakeholder responsibilities for security risks. Section 6 closes the paper with some conclusions.

2. Automated remote pilotage fairway features

This section is based directly on the Sea4Value / Fairway program plan (DIMECC Oy, 2020), which concerns a smart maritime transport system and its automated remote pilotage fairway navigation. This automated fairway navigation ensures a channel by which the existing vessels and future develop of vessels. It enables one path of the digital supply chain. In maritime navigation operations, the sea areas can be distributed to different approach areas of the ports. In the case of fairway navigation, the information requirements and the amount of information needs are related to the accuracy and reliability of safe and efficient fairway navigation. According to the Sea4Value/Fairway research project plan, the main information items required are as follows:

- movement of the ship, particularly the speed and rate of turn (and accuracy of course keeping) and its predicted path
- dimensions and location of the navigable fairway (particularly the limits of the fairway)
- position of the ship and high accuracy of position fixing (need for redundancy in position fixing)
- maritime aids to navigation
- vessel traffic to be encountered and the location of encounter
- environmental conditions
- safety-related communication
- the intended route to destination
- actual route plan to destination including waypoints (wheel over points and turning radius to be used).

(DIMECC Oy, 2020)

Safe navigation in the fairway process requires the combination of accurate and reliable information along with the competence to use it in decision-making and choose the correct action to be taken. The future ePilotage technical environment vision is presented in Figure 1 according to the Sea4Value/Fairway research project plan. It involves intelligent safety equipment, increased situational awareness and a shore pilotage center (DIMECC Oy, 2020).

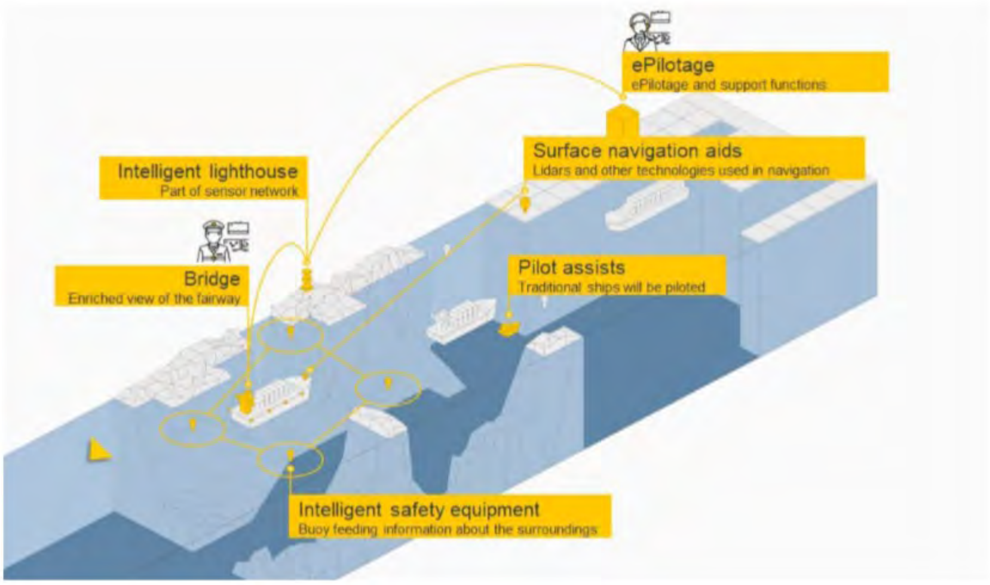
ePilotage
ePilotage and support functions
Surface navigation aids
Lidars and other technologies used in navigation
Intelligent lighthouse
Part of sensor network
Bridge
Enriched view of the fairway
Pilot assists
Traditional ships will be piloted
Intelligent safety equipment
Buoy feeding information about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

Figure 1: Vision of the future ePilotage technical environment (DIMECC Oy, 2020)

It should also be noted that the navigation and pilotage process consist of cooperation and communication among many stakeholders. In the present situation, this is often done by the pilot from the bridge onboard. The relevant stakeholders include:

- law enforcement and maritime authorities
- fairway services ensured by the state (e.g. pilotage and icebreaking)
- commercial fairway and port services (towing, salvage, port, and cargo operations)
- safety authority for weather and sea observations and forecasts.

(DIMECC Oy, 2020)

The list above is not exhaustive and not all stakeholders have a role at all times in the pilotage process. However, it is important to recognize that communication ability must be considered when designing new methods for fairway navigation. This is particularly important with special services, such as towing and icebreaking, as the pilot is often the only person onboard with the competence for using their assistance.

3. Basic elements of cybersecurity for an automated remote piloting fairway

The paper "Basic elements of cybersecurity for an automated remote piloting fairway system" (Pöyhönen, Kovanen & Lehto, 2021) presents a description of a research framework for cybersecurity study of a maritime automated remote pilotage fairway system. It is a combination of a five-layer cyberstructure of an organization (Figure 2) and the maritime security management system (MSMS) with aspects of cybersecurity and the block diagram of an automated remote pilotage system (Figure 3).

In general, an organization's cybersecurity management requires comprehensive awareness on the system level. The awareness of an organization and decision-makers can be seen as system-level awareness arrangement. It is possible to integrate an organization's three decision-making levels into a five-layer cyberstructure (Figure 2) in order to have a comprehensive system view of that organization's cybersecurity environment (Pöyhönen & Lehto, 2020).

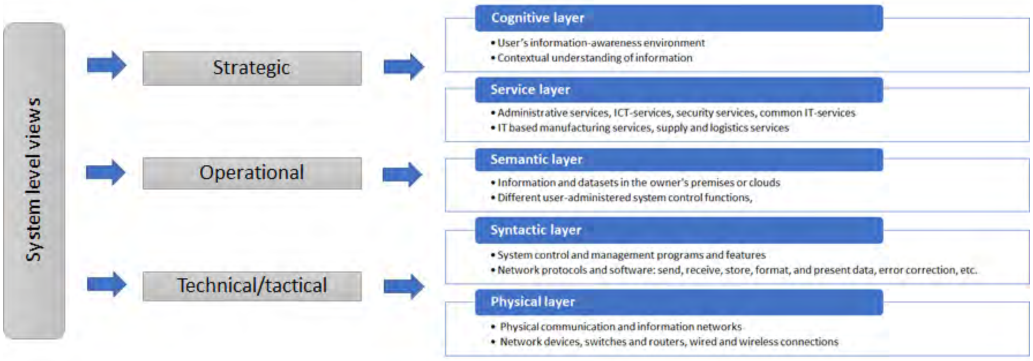
System level views
Strategic
Operational
Technical/tactical
Cognitive layer
• User's information-awareness environment
• Contextual understanding of information
Service layer
• Administrative services, ICT-services, security services, common IT-services
• IT based manufacturing services, supply and logistics 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 2: System-level view of organizational cybersecurity (Pöyhönen & Lehto, 2020)

In the paper "The Maritime Security Management System: Perceptions of the International Shipping Community" (2007), Vinh V. Thai and Devinder Grewal from the Australian Maritime College emphasize the importance of identifying key shore-based and near-shore activities associated with maritime security management. The MSMS includes the following components: activities, main players, organizational relationships, security dimensions, security elements, and criteria. The same basic framework has been used in Sea4Value research. The cybersecurity aspects and features in our research are similar to the activities component, meaning the ePilotage process itself, and security elements, which include capabilities such as people, processes, and technology. These can be seen as common elements in cybersecurity management of the process. The other features of cybersecurity management include security dimensions such as those systems that are needed for operations, security awareness, and training. The risk management and continuity enhancement of system operations establish the criteria for security management. In that sense, the strategy, operational and technology/tactical viewpoints on the systems of stakeholders support a holistic approach to security. The rest of cybersecurity system features include stakeholders and their organizational relationships (Pöyhönen et al., 2021).

Figure 3 presents the cybersecurity system sides as a block diagram for the case of the ePilotage process. The direct and main process systems are fairway systems, ship systems and control center systems. The automated remote pilotage operations also need support processes like vessel traffic service (VTS) and weather forecast services. Situation awareness from other vessels and stakeholder's operation are also essential information and support processes. The complete system is a complex SoS, including information flows between process elements mentioned above with cybersecurity risks (Pöyhönen, et al., 2021).

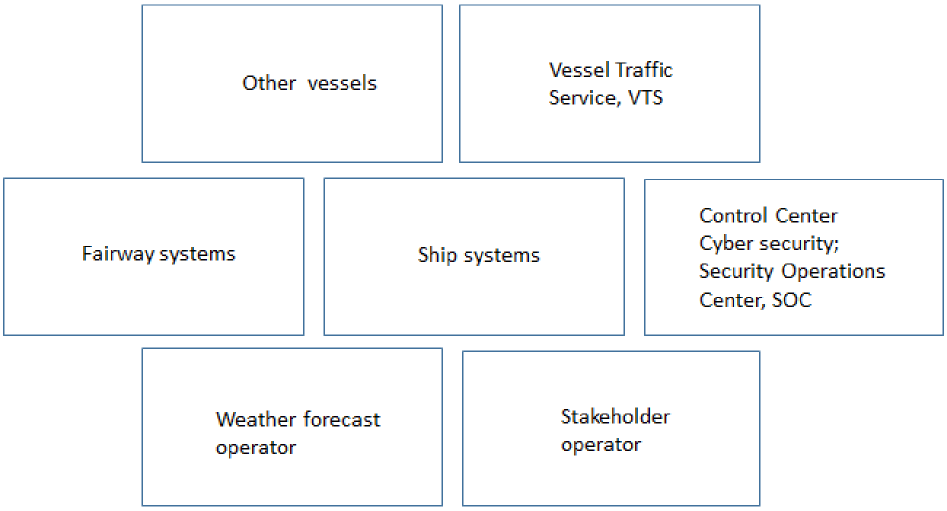
Other vessels
Vessel Traffic Service, VTS
Fairway systems
Ship systems
Control Center Cyber security; Security Operations Center, SOC
Weather forecast operator
Stakeholder operator

Figure 3: Block diagram of an automated remote pilotage system (Amro A., 2019, modified; Pöyhönen, et al., 2021)

4. Risk assessment

The development of ePilotage fairway systems increasingly use ICT systems and ICS systems to exchange information between systems on the navigation process. It happens via different data and communication lines. These information flows use legacy as well as new technologies, which are very important parts of cybersecurity risk analysis work. The recognition of these technologies enables us to identify different functions at the system level, carry out risk assessments and identify their residual risks with sufficient accuracy. In the same way, the dependencies of different information systems need to be considered and, based on these dependencies, security and cybersecurity risks need to be identified. In this chapter we present a probability approach to cyberattacks versus a probability to defend attacks and at the end to evaluate cybersecurity risks related to the information flows of ePilotage operations. We do argue that many previously described detailed calculation principles of cyber-risks, such as the paper "Dynamic Security Risk Management Using Bayesian Attack Graphs" (Poolsappasit, Dewri & Ray, 2012), are too complicated to use in daily life. We thought that there should be a more practical method and tool to make cyber-risk assessments in SoS environments.

A cyber-threat model captures information about potential cyberthreats against a system, an enterprise, an SoS, a region, or a critical infrastructure (CI) sector. A cyber-threat model can serve as a basis for a variety of tasks in different scopes. Comprehensive cybersecurity needs wide scale of analysis of a system of systems (or sub-system) against a set of threat events. It can be often impractical and, in that sense, analysis of system of systems could rely on the development and use of threat scenarios. A threat scenario could include the picture of a potential threat and the result of harmful consequences (Bodeu & McCollum, 2018, 1).

In order to have a practical SoS threat scenario, an adversary can operate by targeting tailored attacks or attacks that reflect the broader scale of the system. Rather than focus only on specific assets or asset types, SoS threat modeling should also focus on sub-sectors or specific business functions. For SoS, three aspects of the scope can be considered (Bodeu & McCollum, 2018, 13):

- Institutional scope: whether the adversary's targeting focuses on a single institution or on a family of institutions.
- Functional scope: how narrowly or broadly a business function, sub-sector, or sector is targeted.
- Technical scope: how specifically or broadly are technologies (or specific systems)
- targeted.

At the strategic level (institutional scope), there must be a description of the situation with non-technical terminology. This includes, for example, discussion of the attacker's motivations by studying different types of adversaries, such as cybercrime or terrorism, etc. At the operational level (Functional scope), there must have a description of the situation with business continuity. This includes, for example, information of the attacker's capabilities to attack against ICT and ICS systems. At the technical/tactical level (Technical scope), there must be more technical information on the threat actor's tactics, techniques, and procedures.

The Bayesian attack graph model have been studied in several areas of security risk management. The paper "Dynamic Security Risk Management Using Bayesian Attack Graphs" (Poolsappasit et al., 2012) proposes a risk management framework using Bayesian networks in order to quantify the chances of network compromise at various levels of system constructions. In the same sense, various threat risk analysis schemes have been developed to recognize the attack and implement the security safeguards to protect the ICT system asset from cyber-attacks (Wang & Liu, 2014): "Attack trees (AT) technique plays an important role to investigate the threat analysis problem to known cyber-attacks for risk assessment". An attack graph is based on a probabilistic metric model and can be used to quantify the cybersecurity issues of an SoS environment.

In this paper, an attack tree graph is used to represent the relationship between threat and defense actions in the ePilotage process. At the SoS level, it is more than a metric model a way of thinking, because there are many layers in the system configuration. Exact probability calculation is therefore complicated, and results can be inaccurate. According to our experiences, as the authors of this paper and other ePilotage research group members, we are familiar with the attack tree graph as a tool for risk assessment. The result of this is representing the likelihood of an attacks against the likelihood of defense against such an attacks. The final probability of success of defense measures versus attacks will be estimated and the most serious attacks will be recognized and prioritized. This probability evaluation work is proposed to be done by cybersecurity experts by utilizing all relevant information that is available from the cybersecurity features of the used technology in the current information flow (see Table 3) and as well as information from stakeholders' capabilities to have defense measures. In this sense we would like to propose the use of Delphi method principle to make relevant threat analysis and risk level estimations from the systems. It is a useful way of thinking about likelihood and probabilities at the system level of a process or an organization.

The risks probability estimation can be extended to the system level as described below. The National Institute of Standards and Technology (NIST) released recommendations as "Framework for Improving Critical Infrastructure Cybersecurity" (2018) for owners and operators of critical infrastructure to help them identify, assess, and manage cyber-risks. The Framework Core part of the guidance has a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Framework Core provide detailed guidance to help an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Framework Core consists of five concurrent and continuous Functions: Identify, Protect, Detect, Respond, Recover. There is mentioned that "The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure" (NIST, 2018).

In this paper, functions according to NIST are proposed to exploit a system risk framework. The meaning of its notations are described in Table 1. Cybersecurity risk assessment can be set to S4F ePilotage process by investigating probabilities and using the elements of the table. In other words, the table can be used as a risk assessment tool by investigating the probabilities of each element of it. After that, it is practical to apply probability tree principles. In Figure 4, the probability tree is described as using Defense probability $P_{D`}$ against Attack probability $P_A$ in the ePilotage process. Cyberattacks (A) in this Sea4Value ePilotage process are the same as the "Attack Identification" and located on all levels of system responsibilities. The $P_A$ attack probability ($P_{SOT}$) to defend attack probability $P_{D`}$ (P_P, P_D, P_M, P_R) is related to the combination of cybersecurity capabilities (people, processes, and technologies) (Jacobs, von Solms & Grobler, 2016), using "Protection" (P), "Detection" (D), "Countermeasure" (M) and "Recovery" activities according to Table 1. The entire risk assessment process needs to have experienced cybersecurity professionals performing this work.

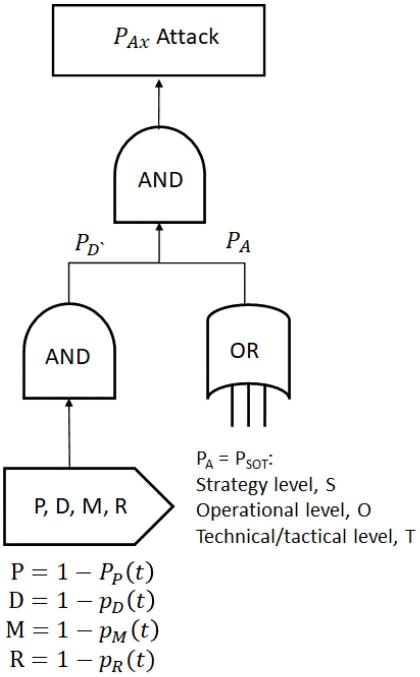
P_{Ax} Attack
AND
$P_{D`}$
P_A
AND
OR
P, D, M, R
$P_A = P_{SOT}$:
Strategy level, S
Operational level, O
Technical/tactical level, T
$\mathrm{P} = 1 - P_P(t)$
$\mathrm{D} = 1 - p_D(t)$
$\mathrm{M} = 1 - p_M(t)$
$\mathrm{R} = 1 - p_R(t)$

Figure 4: Probability tree; Defense probability $P_{D`}$ against Attack probability P_A in the ePilotage process (Wang & Liu, 2014, mod.)

Table 1: Meaning of Notations of ships risk probabilities (NIST, 2018; Hummelholm et al., 2021)

ACTION	**EXAMPLES**	**NOTATION**
ATTACK IDENTIFICATION	1. Attacks at strategy level (S) 2. Attacks at operational level (O) 3. Attacks at the technical/tactical level (T)	A
PROTECTION CATEGORIES	1. Identity Management and Access Control 2. Awareness and Training 3. Data Security 4. Information Protection Processes and Procedures, 5. Maintenance 6. Protective Technology (Port scan, FIREWALL, IDS, IPS, SIEM…)	P
DETECTION GATEGORIES	1. Anomalies and Events 2. Security Continuous Monitoring and Detection a) SOC	D
COUNTERMEASURE (RESPOND) CATEGORIES	1. Conducting Response Planning 2. Communications and Analysis: a) Real time Situation Awareness b) OODA-procedure 3. Mitigation and Improvements	M
RECOVERY CATEGORIES	1. Recovery Planning 2. Improvements 3. Communications.	R

The probabilistic success of attacks, P(t), against the defense of system x can now be evaluated and calculated as follows adapting the principle in "Threat Analysis of Cyber-Attacks with Attack Tree+" (Wang & Liu, 2014, mod.)

$$P_{Ax}(t) = P_A P_{D`} = (P_{SOT})(1 - P_P(t))(1 - p_D(t))(1 - p_M(t))(1 - p_R(t)) \qquad (1)$$

where, as a function of time t, a successful attack against a system x, P_{Ax} has attack success probabilities P_A (P_{SOT}: strategy level S; operational level, O; technical/tactical level, T) reduced by a defending mechanism, $P_{D`}$: protection P, detection D, countermeasure M and recovery R having the respective success probabilities P_P, P_D, P_M and P_R.

Table 2 illustrates the cybersecurity dimensions of systems of the ePilotage process. (Pöyhönen et al., 2021). Table 2 also includes subsystems for information flows and the relevant technologies in the columns. The information technologies behind the numbers are explained in Table 3. The risks assessment process should be based on knowledge of threats, the vulnerabilities of these technologies and the capabilities of relevant stakeholders to recognize and defend the attacks behind the threats.

Table 2: ePilotage system dimensions, an example of subsystem and ICT technologies

ePilotage subsystem	**Ship**	**Other Ships**	**Control Center**	**VTS**	**Weather Forecast**	**Stakeholders**	**Fairway**
AIS	2	2					
Telecomm.	3	3	3	3	3	3	
Weather	1	1	7		7		
Radar	1	1	7				
GNSS	4	4					
Internet	3	3	7	7	7	7	
Cloud	3	3	7	7	7	7	
Drone	3,4,5,6	3,4,5,6					
Fairway sensors	5	5					5

In general, organizations should identify, characterize, and provide representative examples of attacks, and likelihood determinations promote a common terminology and frame of reference for comparing and addressing risks across disparate mission/business areas. Organizations can also select appropriate risk assessment methodologies, depending on organizational governance, culture, and how divergent the missions/business functions are within the respective organizations (NIST 800-39, 2011).

It is proposed that in the ePilotage process, the risk assessment methodology will be based on attack probabilities against probabilities to defend actions of adversarial in communication technologies and thus in information flows between the main system of systems. Table 3 presents a tool to recognize risks by using relevant references. It is also a tool for risk estimation against information flows. Risk assessments can be conducted at any of the process decision levels (Strategy level, S, Operational level, O, Technical/tactical level, T) with different objectives and the utility of the information produced from people, processes, and technology. At the end of the risk assessment work, total risks can be addressed to the security dimensions of the ePilotage process by using Table 2.

Table 3: Risk assessment of information flows

Cybersecurity risks/ **ICT technology**	**Cybersecurity information: References**	**Risk evaluation** **P = act, mot, vul** **D` = defense**
1. VHF/(HF)	Cyberthreats CS feature Situation awareness	P_A=f(S,O,T) D`=f(P,D,M,R)
2. Satellite	Cyberthreats CS feature Situation awareness	P_A=f(S,O,T) D`=f(P,D,M,R)
3. GSM/4G/5G	Cyberthreats CS feature Situation awareness	P_A=f(S,O,T) D`=f(P,D,M,R)
4. GNSS/GPS	Cyberthreats CS feature Situation awareness	P_A=f(S,O,T) D`=f(P,D,M,R)
5. MESH	Cyberthreats CS feature Situation awareness	P_A=f(S,O,T) D`=f(P,D,M,R)
6. WiFi	Cyberthreats CS feature Situation awareness	P_A=f(S,O,T) D`=f(P,D,M,R)
7. Capel network	Cyberthreats CS feature Situation awareness	P_A=f(S,O,T) D`=f(P,D,M,R)

After risk assessment process, ePilotage stakeholders can respond to risks in a variety of ways. These could include risk acceptance, risk avoidance, risk mitigation, risk sharing, risk transfer, or a combination of the above (NIST 800-39, 2011). The stakeholders should monitor ePilotage risks of operations continuously including the purpose, type, and frequency of monitoring activities. Risk monitoring provides stakeholders with the means to verify compliance, determine the ongoing effectiveness of risk response measures, and identify risk-impacting changes to information systems and environments of operation (NIST 800-39, 2011). Analyzing monitoring results allows the stakeholders to maintain situations awareness (SA) by using the risk being incurred, highlight the need to revisit the risk management process, and initiate process improvement activities as needed and communicate with other stakeholders.

5. Discussion

In addition to the attack probability in information flows of the ePilotage process, it is necessary to consider the cybersecurity procedures of ships, every stakeholder and fairway service producer. Threats to information and communication systems and as well as to industrial control systems can include purposeful attacks, vulnerabilities in the systems, and human or machine errors, causing great harm to the services and economy of maritime traffic. Therefore, it is imperative that all stakeholders (Table 2: responsible security dimensions) and at all levels of decision processes understand their responsibilities and are held accountable for managing information security risks. The cybersecurity architecture of stakeholders is an integral part of a comprehensive cybersecurity architecture in any process case (Pöyhönen & Lehto, 2020). It represents system resilience along with providing cybersecurity capabilities for maritime traffic and its operation continuity resilience.

In order to make the piloting process cybersecure, the risks for the main information flows at the SoS level should be investigated carefully. The proposed risk assessment is an efficient method and key element to make threats and defense capabilities visible. Cybersecurity is an essential part of the trust process. The main advantage of the proposed approach is to achieve good results in near real-time effective attack modelling and security evaluation by using constant awareness of threats, vulnerabilities, and defense procedures.

In that sense, all stakeholders should have real-time situation awareness (SA) of the ePilotage process. In addition, they should use an Observe – Orient – Decide – Act (OODA) loop for SA information sharing between each other (Pöyhönen, Rajamäki, Ruoslahti & Lehto, 2020). These are the key features for conducting response procedures to the risk management across ePilotage process.

6. Conclusion

In order to develop maritime autonomy in the first stage in Finland, the Sea4Value / Fairway (S4VF) research program has been launched to create automated remote fairway pilotage features in the near future. ePilotage, the automated remote pilotage system, is a process and an essential part of the critical maritime traffic and transportation supply chain. The fairway and its stakeholders' ICT and ICS systems are together a complex SoS entity, characterized by a conglomeration of interconnected networks and operational dependencies. This new research program increases the amount digital solutions, stakeholders, and subcontractors in maritime fairways. However, there will also be a continuing need for traditional engineering solutions for a long time to come. This development introduces increased risks of a malicious cyberadversary taking deliberate actions against the systems. A comprehensive risk assessment of the ePilotage process should be done according to the principles of SoS modeling.

This paper has established a research framework for the cybersecurity risk assessment of maritime automated remote ePilotage fairway systems and processes. The framework uses probability evaluation in main ICT information flows between the main fairway systems. The risk assessment methodology that has been used is based on attack probabilities against the probabilities to defend against adversarial actions in the use of communication technologies. Risks assessment factors have been identified and the risk assessment tool has been described. It is a way of thinking about risks and risk prioritization. These are needed to answer the research question: "How can the cybersecurity risks of automated remote piloting fairway operations be evaluated?"

Protecting the ePilotage system against cyberthreats implies measures taken based on risk assessment, and they ensure confidentiality, integrity, and the availability of primarily digital information in the operating processes being examined. The measures should be highly significant for the overall availability of the systems that support the stakeholders' processes in the ePilotage environment. Operational availability plays a key role in achieving operational continuity and promoting the reliability of activities. Cybersecurity risk management and information security are mandatory features from the point of view of operational trust, continuity, reliability, and resiliency.

References

Amro, A. (2019). Communication and Cybersecurity for Autonomous Passenger Ferry (Autoferry).

Bodeu, D. J. & McCollum, C. D. (2018). System-of-systems threat model. The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE: Bedford, MA, USA

DIMECC Oy, 2020. Sea4Value / Fairway program (S4VF).

Finnpilot Pilotage Ltd, (2020). https://finnpilot.fi/en/pilotage/what-is-pilotage/

EU Commission, 2009. Critical information infrastructure protection (2009), COM (2009) 149 final, Commission of the European Communities, Brussels, 30.3.2009.

Hummelholm, A., Pöyhönen, J., Kovanen, T. & Lehto, M. (2021). Cyber Security Analysis for Ships in Remote Pilotage Environment. Submitted to be published in ECCWS 2021 - 20th European Conference on Cyber Warfare and Security. 24th - 25th June 2021, Chester, UK.

Jacobs, P. C., von Solms, S. H. & Grobler, M. M. (2016). Towards a framework for the development of business cybersecurity capabilities. International Conference on Business and Cyber Security (ICBCS), London, UK. The Business and Management Review, Volume 7 Number 4, 51–61.

Kovanen, T., Pöyhönen, J. & Lehto M. (2021a). ePilotage System of Systems' Cyber Threat Impact Evaluation. Proceedings of the 16th International Conference on Cyber Warfare and Security ICCWS 2021. p. 144-151.

Kovanen, T., Pöyhönen J. & Lehto M., (2021b). Cyber Threat Analysis in the Remote Pilotage System. Submitted to be published in ECCWS 2021 - 20th European Conference on Cyber Warfare and Security. 24th - 25th June 2021, Chester, UK.

National Institute of Standards and Technology, NIST 800-39, (2011). Managing Information Security Risk. Organization, Mission, and Information System View. U.S. Department of Commerce

National Institute of Standards and Technology, NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018

Poolsappasit, N., Dewri, R. & Ray, I. (2012). Dynamic Security Risk Management Using Bayesian Attack Graphs. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, JANUARY/FEBRUARY 2012

Pöyhönen, J., Rajamäki, J., Ruoslahti, H. and Lehto, M. (2020). Cyber Situational Awareness in Critical Infrastructure Protection. Article approved 2nd March 2020 to Cyber Security of Critical Infrastructure 2020 (CYSEC2020) conference, October 27th, 2020 - October 28th, 2020. Dubrovnik. Croatia.

Pöyhönen J. & Lehto M. (2020). Cyber security: Trust based architecture in the management of an organization security. The 18th European Conference on Cyber Warfare and Security ECCWS2020, 25-26 June 2020, University of Chester, UK, pages 304-313

Pöyhönen J., Kovanen T. & Lehto M., (2021). Basic elements of cyber security for an automated remote piloting fairway system. Proceedings of the 16th International Conference on Cyber Warfare and Security ICCWS 2021. p. 299-308.

Thai, V.V & Grewal, D. (2007). The Maritime Security Management System: Perceptions of the International Shipping Community. Article in Maritime Economics & Logistics · June 2007.

Wang, P. & Liu, J. C. (2014). Threat analysis of cyber-attacks with attack tree+. Journal of Information Hiding and Multimedia Signal Processing, 5(4).