Cybersecurity Risk Assessment Subjects in Information Flows

Jouni Pöyhönen, Aarne Hummelholm and Martti Lehto
Faculty of Information Technology, University of Jyväskylä, Finland
aarne.hummelholm@elisanet.fi
jouni.a.poyhonen@jyu.fi
martti.j.lehto@jyu.fi

Abstract: A modern society includes several critical infrastructures in which digitalization can have positive impacts on the levels of autonomy and efficiency in the use of infrastructure systems. Maritime transportation is an example of an infrastructure that currently needs development in the digitalization of its operations and processes. At the same time, maritime processes represent a large-scale cyber environment, thus trustable information distribution between system elements of the processes is needed. Since 2020, the Sea4Value / Fairway (S4VF) research program in Finland has been working to develop maritime digitalization which can lead to autonomy processes in the future. The first stage of the program has led to a demonstration phase of remote fairway piloting. This remote fairway piloting process, "ePilotage," is a complex system-of-systems entity. In this entity, fairway systems, ship systems and control center systems are the main processes from the operational point of view. Remote pilotage operations need support processes such as vessel traffic service (VTS) and weather forecast services. Situation awareness from other vessels and the stakeholder's processes are also essential information for the entire piloting operation. In this context, a new concept of information flows at the technical level will be based partly on cloud servers. In this paper, a cybersecurity risk assessment has been carried out at the technical level of information and communication technologies (ICT), and it concerns information transmission between a ship and a cloud server. It describes the most important topics for a comprehensive risk assessment in a specific ship-to-cloud information flow of the fairway process. The findings of the study can be considered good examples of the management of cybersecurity risks in critical information flows between all main system blocks of the fairway process. The research question is as follows: "How can the cybersecurity risks of information flows in a system-of-systems entity be described and evaluated?" The main findings are related to the risks of transmitting information from a ship to a cloud server. The methodology that has been used is based on analyzing the probabilities of cyberattacks occurring in relation to the probabilities to defend against these actions. The main risk assessment topics have been listed.

Keywords: maritime digitalization, cybersecurity, information flow, risk topics

1. Introduction

As the first stage in developing maritime autonomy in Finland, the Sea4Value (S4V) research program was started in 2020. The program is now becoming a research program of digitalization of harbor processes. At the beginning of the program, the research concentrated on creating automated remote pilotage fairway features (ePilotage). The ePilotage Act refers to the digitalization of activities related to the remote navigation of vessels on local waters. The purpose of this was to enhance the safety of vessel traffic and prevent environmental damage generated by vessel traffic (Finnpilot Pilotage Ltd, 2020).

Finnpilot Pilotage (2020) defines pilotage as follows: "As defined in the Pilotage 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." The mission of the Sea4Value / Fairway (S4VF) program is to enhance towards digitalization, service innovation and information flows in maritime transport in order to prepare for advanced autonomous operations and navigation as a long-term mission. A key step towards an autonomous transport system is to ensure safe, sustainable, and efficient channel for ships to enter and leave harbors. The S4VF program improves the safe navigation for existing vessels and lays the system-of-systems foundation for autonomous vessels of the future. The ePilotage process as a remote pilotage fairway is the first step in this way.

The ePilotage environment of the S4FV project is an example of a system-of-systems in which an increased number of digital solutions are entering new environments where traditional engineering solutions are still in use. This development introduces increased risks of a malicious cyber adversaries taking deliberate actions against the system. For this reason, the threat analyses should be carried out according to the principles within the scope of the "system-of-systems threat model" (Bodeau & McCollum, 2018).

This paper describes a risk assessment approach for the remote pilotage system-of-systems environment and related threats by using an example of a subsystem and utilizing the Mitre ATT&CK framework. A remote pilotage system-of-systems configuration includes both ICT and industrial control systems (ICS) networks and components.

In this paper, cybersecurity risk assessment has been carried out on an organization's technical level as an example of the importance of trustworthy information chains in the system-of-systems architecture. It concerns information flow from a ship to a cloud server. One of the ways to use this information is to control the ePilotage process. This paper follows our previous papers on the S4V research program and describes the most important topics for comprehensive risk assessment in specific cloud information flows of the fairway process. The findings of the study can be considered good examples of cybersecurity risk assessment work in critical information flows between the main system blocks of the fairway process. The research question is as follows: "How can the cybersecurity risks of the main information flows in a system-of-systems entity be described and evaluated?"

The main findings are related to the risks of transmitting essential process information from a ship to a cloud server. The methodology used is based on analyzing the probabilities of a cyberattack in relation to the probabilities to defend against such actions in the use of ICT. The main risks assessment topics have been listed.

2. System-of-systems ICT network architecture and general attack vectors

Figure 1 shows the general communication network architecture and the main attack vectors related to the architecture. In this context, ship systems are like a home, factory, and so on. Ships and ship systems are important parts of the ePilotage process because they are remote pilotage attributes. At the same time, ships are connected to land-based communication and control systems and satellite systems. In this case, the ship is connected to land-based control systems via the cloud. The ship systems are also vulnerable to cyber-attacks in a similar way as other ICT and ICS systems, applications and devices are. Attacks can come from either inside the ship or outside the ship. Cyber-attackers can harm the control information that is needed for operations. The main attack vectors at the system level are shown in Figure 1.

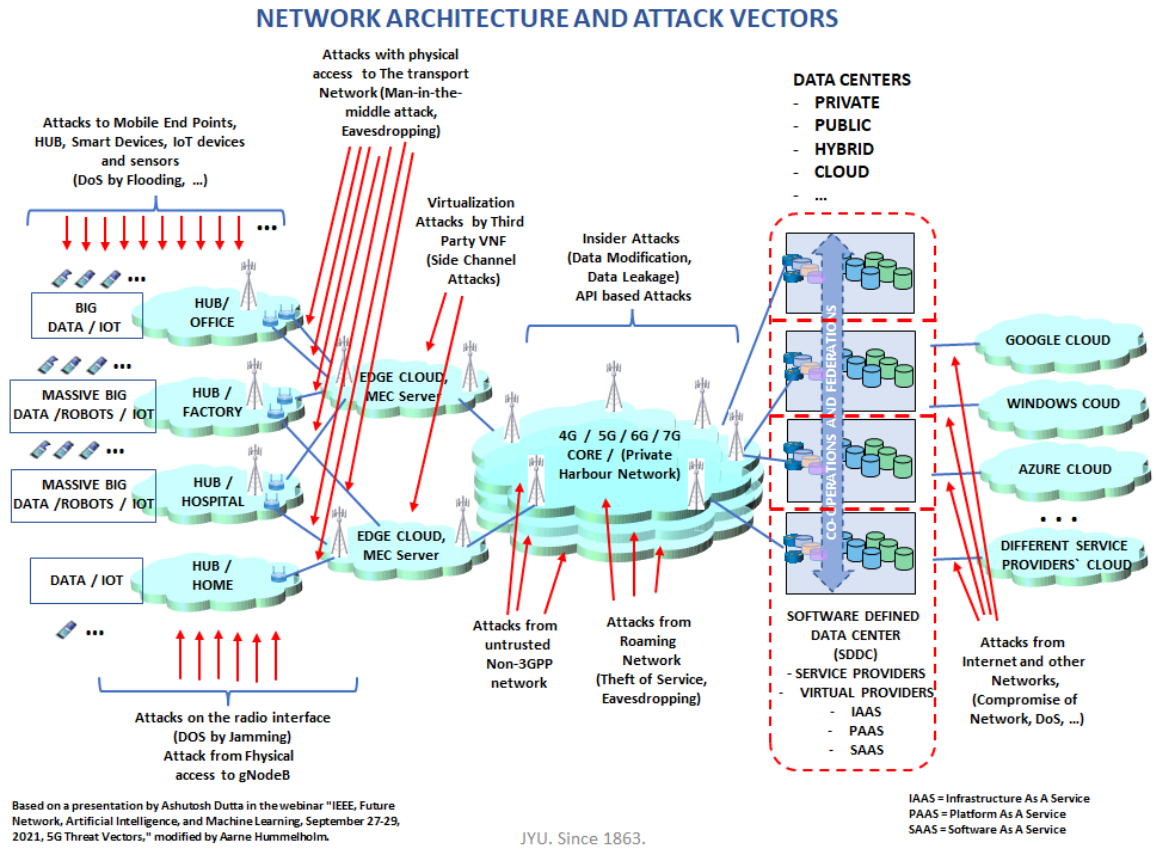

Figure 1: System-of-systems communication network architecture and the main attack vectors (Dutta, 2021, modified)

Understanding the motivation aspect enables situations that heighten the risk of a cyber-attack to be predicted (Casey, 2015). By combining the motivational factors for each attack archetype, it is possible to discover different events being triggered by attacks. Many cyber-attacks are associated with social, political, economic, and cultural backgrounds. It is crucial to identify comprehensively different kinds of circumstances that might trigger an attacker archetype. This can be valuable for risk assessments related to various situations. The motivation affects the attacker's targeting and methods. A vandal seeks visibility by defacing a website, but a spy wishes to stay unnoticed to gain information. The varying level of capability restricts some of the attackers from achieving their goals (Bodeau, McCollum & Fox, 2018). Therefore, being motivated does not mean that an attack is possible for the attacker. Understanding the motivations and capabilities of different archetypes limits the number of scenarios and thus makes evaluation feasible for the defender.

In the case of cybervandalism, the arrival of a controversial ship in a fairway might trigger actions mainly from ideological motivations. The controversy might be with the cargo, the ship's operations, or the owner. For cybercrime, valuable cargo is more tempting because financial gains act as the motivation. Cyberterrorism or sabotage can include business or political motivations. Political factors may arise from national or international issues. In the worst case, international tensions in the region could escalate to military cyber operations against maritime traffic. The parameters of the attacker archetypes for this case are presented in Table 1. (Kovanen, Pöyhönen & Lehto, 2021a)

Table 1: Attributes of the attacker archetypes (Kovanen, Pöyhönen & Lehto, 2021 a)

	Vandalism	Crime	Terrorism	Sabotage
Motivation and goal	Trying to make political change based on personal political or ideological motives. Egoism gain	Making money through fraud or from the sale of valuable information. Financial gain	Gaining social instability and influencing political decision-making. Anarchy gain	Causing instability, chaos, political change, and infrastructure paralysis. Paralysis gain
Target	Digital services of governments and companies, individuals' information systems	Digital services of governments and companies, individuals' information systems	Data and information about governments and companies. Critical infrastructure	Nation's critical infrastructure
Impacts	ICT: Defacement ICT: Network Denial of Service ICS: Loss of Productivity and Revenue	ICT: Data Encrypted for Impact (ransom) ICT: Resource Hijacking (mining cryptocurrencies) ICS: Manipulation of Control	ICS: Loss of Safety	ICS: Damage to Property (shipwreck)

3. The study of ship information

In many ways, the cyberworld challenges organizations, processes, and the use of technologies. An organization can use its own capabilities to develop security in its cyber domain. They can do so by enhancing its capabilities that are applicable to the operational domain. These can consist of people, processes, and technology meant to achieve outcomes or effects (Jacobs, von Solms & Grobler, 2016). It important to note that these capabilities can also include cyber vulnerabilities.

The remote pilotage process, ePilotage, is a special environment with a large network of separate systems and stakeholders in the cyber domain. By examining the impacts of cyberthreat actions and thus risks assessment in this connected environment, it is obvious that the threat impacts affecting one subsystem are propagated to affect other systems. For that reason, people, processes, and technologies should all be considered in risk assessment work, even if we have just one organization's technical level under risk evaluation.

3.1 People: Stakeholders

Management must recognize that clear, rational, and risk-based decisions are necessary from the point of view of process continuity. Understanding and dealing with risks are part of an organization's strategic capabilities and key tasks when organizing the operations. This requires, for example, the continuous recognition and understanding of security risks at the different levels of management. The security risks may be targeted not

only at the organization's own operation but also at individuals, other organizations, and society as a whole—and in this case the entire ePilotage process. (Joint Task Force Transformation Initiative, 2011) The Joint Task Force Transformation Initiative (2011) recommends implementing an organization's cyber risk management as a comprehensive operation, in which the risks are dealt with from the strategic to the tactical level. In this way, risk-based decision-making is integrated into all parts of an organization. In research by the Joint Task Force Transformation Initiative, the follow-up operations of the risks are emphasized on every decision-making level. For example, on the tactical level, the follow-up operations may include constant threat evaluations about how the changes in an area can affect the strategic and operational levels. The operational level's follow-up operations, in turn, may contain, for example, the analysis of new or current technologies in order to recognize the risks to business continuity. The follow-up operations on the strategic level can often concentrate on an organization's information system entities, the standardization of the operation and, for example, on the continuous monitoring of the security operation. (Joint Task Force Transformation Initiative, 2011)

3.2 Process: ePilotage, (subprocess: Ship information flow)

ENISA emphasizes maritime transport as a crucial activity for the European Union economy. The global digitalization trend has led authorities to set recent policies and regulations to maritime processes to face new cybersecurity challenges with regards to IT and ICT (ENISA, 2019). Development, implementation, and maintenance of a cyber risk management program is essential part of organizations processes. The management of the process by the organizations senior experts should stay engaged to it throughout the process to ensure that the protection and contingency planning are balanced to manage risks within an acceptable limit (BIMCO et al., 2021). Processes are key to the implementation of an effective cybersecurity strategy. Processes are crucial in defining how the organization's activities, roles, and documentation are used to mitigate the risks to the organization's information. Processes also need to be continually reviewed: cyberthreats change quickly, and processes need to adapt with them. Processes, however, are nothing if people fail to follow them correctly (Dutton, 2017).

3.3 Technology: Ship systems, ICT-systems, Cloud Service

Technology is obviously crucial when it comes to cybersecurity at the organization's tactical level. By identifying the cyber risks that an organization faces, it can then start to look at what controls to put in place, and what technologies will be needed to do this. Technology can be deployed to prevent or reduce the impact of cyber risks, depending on your risk assessment and what you deem an acceptable level of risk (Dutton, 2017). Figure 2 presents the current technology at the subsystem level of information and information flow from ship to cloud and after that in use by the remote control center (RCC). Data storage in cloud and cloud computing services are used also for many other purposes of the remote pilotage process. The detailed configuration on the technical level is described Figure 3. Cloud computing services are platforms of two-sided markets connecting users with developers of complementary products or services. The resultant user-side transactions allow providers of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). (Arce, 2020)

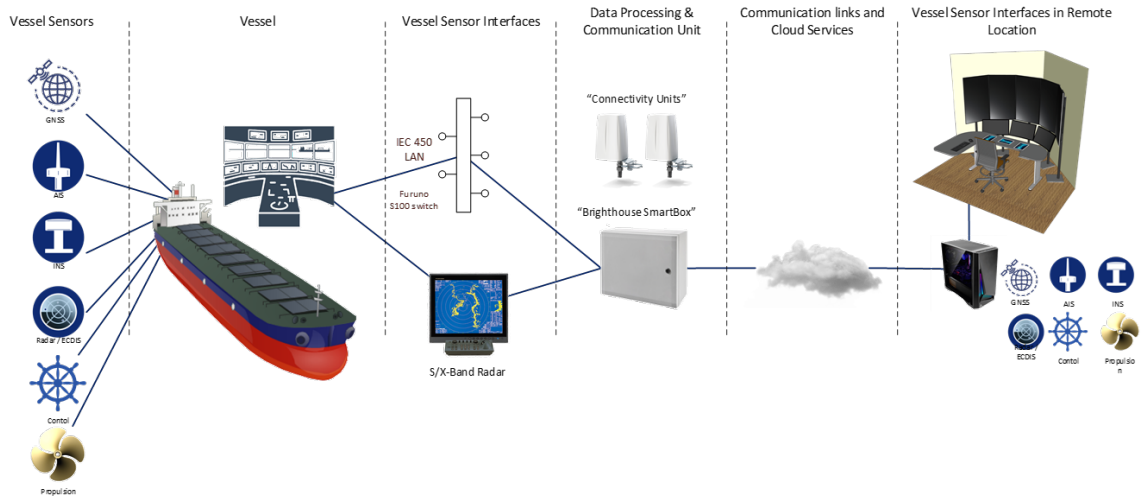

Figure 2: Ship sensors' information flow to the control center (Brighthouse Intelligence, 2021)

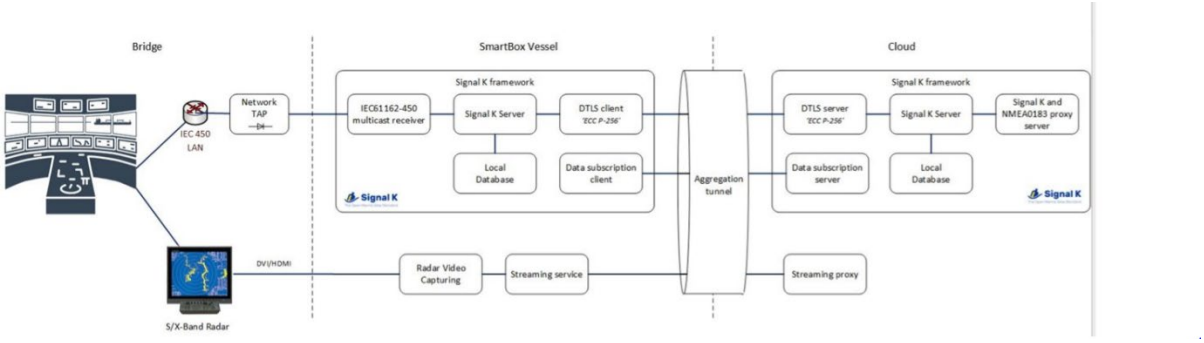

Figure 3: Ship sensors' connection to cloud, communication technology (Brighthouse Intelligence, 2021)

These two figures present the subsystem components of information flow for risk assessment work. These are ship network, ship LAN/WLAN, ship data process, transmitting tunnel, transmitting 4G or 5G, and cloud service. The information flow consists of data from ship status and live camera pictures.

4. Risk assessment method

In this paper, cybersecurity risk assessment has been applied to ship sensor information flow by investigating probabilities and using the elements in Table 2. This method is described in our paper "Assessment of cybersecurity risks: Maritime automated piloting process" (Pöyhönen & Lehto, 2022). The table has been used as a risk assessment tool by investigating the probabilities of each element of it. Probability tree principles have been applied as well. In Figure 4, the probability tree is described as using Defense probability $P_D`$ against Attack probability P_A in the evaluation process. Cyberattacks (A) in the Sea4Value ePilotage process are the same as the "Attack Identification" and located on all levels of the stakeholder's responsibilities (Strategy, Operational, Tactical/Technical) concerning the ship sensor information transmission to the cloud. The P_A attack probability (P_{SOT}) to defend against attack probability $P_D`$ (P_P, P_D, P_M, P_R) is related to the combination of cybersecurity capabilities (people, processes, and technologies), using "Protection" (P), "Detection" (D), "Countermeasure" (M) and "Recovery" (R) activities according to Table 2. The entire risk assessment process has been done by experienced cybersecurity professionals related to the case.

Table 2: Ships risk probabilities (NIST, 2018; Hummelholm, Pöyhönen, Kovanen & Lehto, 2021)

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

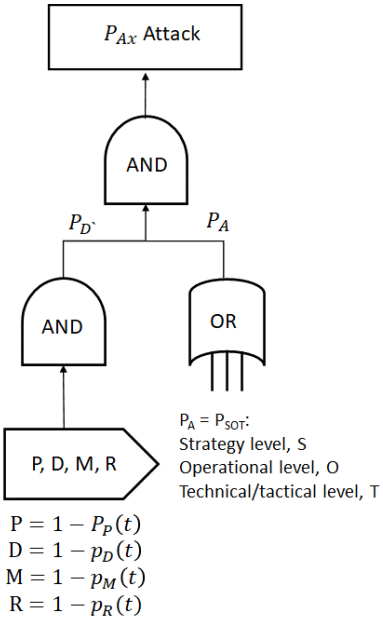

Figure 4: Probability tree; Defense probability $P_{D`}$ against Attack probability P_A in the ePilotage process (Wang & Liu, 2014, Pöyhönen & Lehto, 2022)

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.)

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

5. Making threat analyses and risk levels estimation

In this case we have used Delphi method principle in order to make relevant threat analysis and risk-level estimations from the ship camera system. The members that have been involved in this analysis process are researchers and research methods. Delphi is advocated by cybersecurity experts from the S4V program: "The Delphi method is an iterative process to increase consensus-building and at the end to have consensus among an experts from an examine case. The Delphi method is part of quantitative as a means to achieve an optimally reliable expert consensus." It could have on one of three objectives (Garson, 2012):

- 1. forecasting future events
- 2. achieving policy consensus on goals and objectives within organizations or groups
- 3. identifying diversity in and obtaining feedback from stakeholders in some policy outcome.

Table 3 includes the results of Delphi method research on the ship-to-cloud subsystem. It has been done in order to forecast future events conducted as part of the risk evaluation process. Cybersecurity researchers and expert's contributions are related to the main threats/attacks, the impacts of them, the main defense categories and risk level columns. The probability estimation has been done by the cybersecurity researchers and experts according to the formula (1) principal. In this evaluation it is expected that stakeholders have normal cybersecurity solutions and procedures in use. We have used the OWASP Risk Rating Methodology to identify a security risk. The evaluation has collected information about the threat agent involved, the attack that will be used, the vulnerability involved, and the impact of a successful exploit on the operation of the system. The risk levels are divided into three categories (LOW, MEDIUM, HIGH) depending on the estimated severity of the attack impacts and occurrence of harm after estimated defense capabilities. The determination of the risk level is based on elements within each factor, such as the motive and ability of the attacker, the ease of finding vulnerabilities, the loss of the CIA, and damages to the system. Each factor has a set of options, and each option has a likelihood rating from 0 to 0,9 associated with it. The 0-to-0,9 scale is split into three parts: 0 to <0,3 = LOW, 0,3 to <0,6 = MEDIUM, and 0,6 to 0,9 = HIGH (OWASP, 2022).

Table 3: Ship systems to cloud service; main threats/attacks, related impacts (Mitre, 2019, 2020; Kovanen, Pöyhönen & Lehto, 2021b), main defense categories (NIST, 2018) and risk levels

Subsystem/ Ship-to loud	Main threats/attacks	Impacts	Defense Categories	Risk level
Ship Network	Brute Force Credential Theft	Manipulation of View Denial of Service System Shutdown	Identity Management and Access Control Security Continuous Monitoring and Detection	LOW
Ship LAN or WLAN	Man in the Middle Jamming	Denial of Service	Data Security	MEDIUM
Ship, Data process	Physical Access	Service Stop	Access Control	LOW
Transmitting Tunnel	Credential Theft	Loss of Safety	Identity Management and Access Control	LOW
Transmitting 4G or 5G, 3rd party	Insider Attacks Attacks from Rooming Network API based Attack	Data Destruction Denial of Service	Identity Management and Access Control Communications and Analysis	MEDIUM
Cloud service, 3rd party	Attacks from Internet Insider Attacks Credential Theft DoS Attacks API-based Attack Ransomware Attacks	Data Manipulation Data Destruction Denial of Service Data Encrypted for Impact	Data Security Communications and Analysis Recovery Planning Awareness and Training Security Continuous Monitoring and Detection	HIGH

In an ICS environment, the Mitre framework uses the terms *denial*, *loss*, and *manipulation*. Denial is a condition which occurs only while the attack is active. Loss refers to sustained loss of an asset that continues after the active malicious interaction has ceased. Manipulation alters the asset and can be either loud and easy to detect or subtle and longer sustained. According to the paper "Cyber-Threat Analysis in the Remote Pilotage System" (Kovanen, Pöyhönen & Lehto, 2021b), we have described the impacts as follows:

- **Manipulation of view** is a more subtle attack type than denial or loss of view. Slightly falsified data are harder to detect than missing data. Therefore, the attack can continue for longer periods of time undetected. Consequently, the operator of the affected system loses correct situational awareness and makes decision based on false data. The effect spreads to all connected systems and operators using the manipulated view.
- **Denial of Service** attacks can be carried out by affecting the endpoint or the network that leads there. In either case, the service is unavailable for use. All other systems that depend on the affected system experience difficulties. If an alternative system is available and the deployment is designed and implemented, the effects of this attack type decrease.
- **Data destruction**, as well as **data encrypted for impact**, disk wipe and **service stop**, all prevent the use of the data and services. These can also prevent the use of the whole system in case the action is targeted at, for example, disk structure rather than the data itself. **System shutdown**/reboot can be used to make systems inaccessible faster by, for example, rebooting after wiping the master boot record. The severity of this type of an event depends on the system and time the restoration from backups takes. If similar data or service is served from alternative systems, the overall resilience increases.
- **Loss of Safety** is dangerous especially with cyber physic systems as the result may cause injuries or death when the safety mechanism of a system is disabled. Even a threat of this type of circumstance can delay reaction to other impact types if a human operator is not able to initiate countermeasures due to a fear of unsafe working conditions.
- **Data manipulation** is harder to detect than data destruction if the manipulation is subtle. Systems and operators can continue to act but they base their decisions on false data. For example, location information could be manipulated to lead a ship off course. Depending on the magnitude of the manipulation and the availability of location information from unaffected systems (and the correct comparison checks), the time until detection varies.

Table 4 illustrates the risk levels after the evaluation process in three categories (LOW, MEDIUM, HIGH), selected defense categories, recommendations for relevant risk-level mitigations, and recommendations for action priority. Recommendation priorities are (1) direct, (2) as soon as possible, and (3) when the action is convenient to perform. The action to be taken can be reasonably divided into development circles. The residual risks should be evaluated after the first round and beyond that after every round.

Table 4: Ship system to cloud Service; risk-level mitigation, action priority

Subsystem/ Ship to Cloud systems	Risk level	Defense Categories	Risk level mitigation	Action priority 1–3
Ship Network	LOW	Identity Management and Access Control Security Continuous Monitoring and Detection	Network Segmentation Role Based Access Control Ports Hardening	3
Ship LAN or WLAN	MEDIUM	Data Security	Authentication Policy Access Control WPA2+PSK Security	2
Ship, Data process	LOW	Access Control	Physical Security	1
Transmitting Tunnel	LOW	Identity Management and Access Control	Multi-Factor Authentication VPN update procedure	3
Transmitting 4G or 5G, 3rd party	MEDIUM	Identity Management and Access Control Communications and Analysis	Service Agreement Audit of Service	2
Cloud service, 3rd party	HIGH	Data Security Communications and Analysis Recovery Planning Awareness and Training Security Continuous Monitoring and Detection	Zero Trust Network Access Service Agreement Audit of Agreement	1

Protective technology (Port scan, FIREWALL, IDS, IPS, SIEM) and update procedures of these solutions as well as other relevant resiliency actions, such as cybersecurity policies, are needed in daily life as well as in the use of the ICT environment. In addition to these actions, however, mitigation of the risks identified in Table 4 is highly recommended. These actions may require special attention from every stakeholder of ship information transmission. The priority 1 actions should be performed as soon as possible in the first round of cybersecurity development of ship information flow. This category includes either critical actions or actions that are very easy to perform. The other priorities can be addressed after the first round of development actions, depending on the resources for the development. Residual risks should be determined after every development round.

6. Conclusion

In the first stage of Finnish maritime digitalization, the Sea4Value / Fairway (S4VF) research program has been launched to create automated remote fairway pilotage features. It is called the ePilotage research process. This process is an essential part of the critical maritime traffic and transportation supply chain. The fairway and its stakeholders' systems are together a complex system-of-systems entity, characterized by a conglomeration of interconnected networks and operational dependencies. The research program increases the level of various digital solutions, stakeholders, and processes in maritime fairways. However, there will also be a continuing need for traditional engineering solutions for a long time to come. This environment increases the risks of all levels of people, processes, and technology.

A system-of-systems technical environment is a comprehensive cybersecurity entity, and it should be considered as a common structure for all operationally related stakeholders of the pilotage process. Therefore, in this maritime research case concerning the information flow of ship sensors the systems communication way between process elements is used as example. In this risks assessment evaluation work, we have viewed all risks in such a way that they can been seen as well as the same way between other information flows as they relate to secure communication. In that sense, the paper exploits the risk assessment method where cyberthreats are considered in relation to defense capabilities.

This paper has established a research framework for the cybersecurity risk assessment of maritime automated remote ePilotage fairway systems and processes. The case of the framework is an example and uses risk probability evaluation in one of the most important 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. Risk 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 system-of-systems environment against its cyberthreats implies measures taken based on risk assessment of the system-of-systems, and eventually all critical information flows between those elements. It ensures confidentiality, integrity, and the availability of primarily digital information in the operating processes, achieving operational continuity and the reliability of activities being examined.

References

Arce, G. D. (2020). Cybersecurity and platform competition in the cloud. Computers & Security 93 (2020) 101774.

BIMCO, INTERCARGO, INTERTANKO, ICS, IUMI, OCIMF, OCIMF, Sybass and WORLD SHIPPING COUNCIL (2021). The Guidelines on Cyber Security Onboard Ships. Version 4. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships, retrieved 1.3.2022

Brighthouse Intelligence, (2021). Future Fairway Flash Event, Sea4Value Fairway project report 19.11.2021.

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

Bodeau, D.J., McCollum, C.D. and Fox, D.B. (2018) "Cyber Threat Modeling: Survey, Assessment, and Representative Framework", Mitre Corp, Mclean.

Casey, T. (2015) "Understanding Cyber Threat Motivations to Improve Defense", Intel White Paper.

Dutta, A. (2021) Future Network, Artificial Intelligence, and Machine Learning. IEEE webinar. September 27-29. 2021.

Dutton, J. (2017) Three pillars of cyber security. Available from: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security, retrieved 25.1.2022

ENISA. (2019). *PORT CYBERSECURITY*. Good practices for cybersecurity in the maritime sector. November 2019.

Finnpilot Pilotage Ltd, (2020). Available from: https://finnpilot.fi/en/pilotage/what-is-pilotage/, retrieved 25.1.2022

Garson, G. D. (2012). The Delphi method in quantitative research. Asheboro, NC: Statistical Associates Publishers. Available from: https://faculty.chass.ncsu.edu/garson/PA765/delphi.htm, retrieved 25.1.2022

Hummelholm, A., Pöyhönen, J., Kovanen, T. & Lehto, M. (2021). Cyber Security Analysis for Ships in Remote Pilotage Environment. Presented of 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.

Joint Task Force Transformation Initiative, (2011). NIST Special Publication 800-39: Managing Information Security Risk - Organization, Mission, and Information System View, Gaithersburg: National Institute of Standards and Technology.

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

Kovanen, T., Pöyhönen, J. & Lehto, M. (2021 B). ePilotage System of Systems' Cyber Threat Impact Evaluation. Proceedings of the 16th International Conference on Cyber Warfare and Security ICCWS p. 144-153.

Mitre. (2019). "Impact", Available from: https://attack.mitre.org/tactics/TA0040/, retrieved 25.1.2022

Mitre (2020). Impact. Available from: https://collaborate.mitre.org/attackics/index.php/Impact, retrieved 25.1.2022

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

OWASP Risk Rating Methodology, Available from: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology, retrieved 25.1.2022

Pöyhönen, J. & Lehto, M., (2022). Assessment of cybersecurity risks - Maritime automated piloting process. Submitted to be published in ICCWS 2021 - 17th International Conference on Cyber Warfare and Security. 17th - 18th March 2022, Albany, New York, USA.

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