SINTEF

2021:00341- Unrestricted

CySiMS-SE

D2.2 Updated cyber risk assessment for the maritime industry

Author(s)
Per Håkon Meland
Karin Bernsmed
Egil Wille
Ørnulf Jan Rødseth
Dag Atle Nesheim

KONGSBERG SINTEF NAVTOR KYSTVERKET The Research Council of Norway

SINTEF Digital
SINTEF Digital
Address:

NO-
NORWAY
Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

CySiMS-SE

D2.2 Updated cyber risk assessment for the maritime industry

KEYWORDS:
Cyber security, maritime, cyber threat, risk assessment

VERSION	DATE
1.0	2021-03-25

AUTHOR(S)
Per Håkon Meland
Karin Bernsmed
Egil Wille
Ørnulf Jan Rødseth
Dag Atle Nesheim

CLIENT(S)	CLIENT'S REF.
The Research Council of Norway	CySiMS SE (295969)

PROJECT NO.	NUMBER OF PAGES/APPENDICES:
102019295	22

ABSTRACT

Abstract heading

This report presents an updated assessment of the cyberthreat landscape in the context of CySiMS-SE. It is based on the previous work from CySiMS "D1.1 Risk Model and Analysis" and the methodology from CySiMS-SE "D2.1 Expanded risk and CBA methodology". The goal has been to show how we obtain required means and opportunities of attack vectors for the PKI and motivation factors for potential threat actors.

PREPARED BY Per Håkon Meland	SIGNATURE Per Håkon Meland
CHECKED BY Ravi Borgaonkar	SIGNATURE Ravi Borgaonkar
APPROVED BY Maria Bartnes	SIGNATURE Maria Bartnes

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
2021:00341	978-82-14-06467-4	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2021-03-25	First public version.

Table of contents

1 Introduction

The maritime sector and infrastructure are critical to Norway, EU and the world economy. Digital technology for ships is in continuous development, and cyber security is an important enabler to ensure safe and reliable operations. Cyber Security in Merchant Shipping (CySiMS) (2015-2018) was a Research Council of Norway funded project, which designed security solutions to protect digital communication in the maritime domain. The results have been met with much interest in the maritime community, but there is now an urgent need to develop the specifications from the CySiMS project into a complete system.

The underlying idea of CySiMS-SE is to *demonstrate and operationalize a secure communication solution for the maritime sector and integrating this with the onboard computer architecture*. The solution will include a Public Key Infrastructure (PKI) and necessary hardware and software for secure information exchange across systems on the bridge, off-bridge and on shore. This will provide the world's first open, integrated, and cost-effective protection against cyber-attacks on critical safety and operational information, while contributing to preserving Norway's position as a leading seafarer nation leading the way in developing, adopting and selling technological innovations.

This report presents an updated assessment of the cyberthreat landscape in the context of CySiMS-SE. It is based on the previous work from CySiMS “D1.1 Risk Model and Analysis” [1] and the methodology from CySiMS-SE “D2.1 Expanded risk and CBA methodology” [2]. The goal has been to show how we obtain required means and opportunities of attack vectors for the PKI and motivation factors for potential threat actors.

2 The maritime cyberthreat landscape

The scope of our analysis is the maritime PKI processes and technology stemming from CySiMS and CySiMS-SE. However, this is a new system yet to be fully realised, and it is therefore useful to look at work related to the wider maritime cyberthreat landscape.

During the autumn of 2020, a study on historical incidents and threats in the maritime sector was performed by SINTEF on commission by the Norwegian Coastal Administration. The report [3] from this work is publicly available (in Norwegian) and gives an overview of:

- Ship systems, communication channels and related infrastructure onshore.
- Previous work on assessing maritime threats and vulnerabilities.
- An overview of 35 known cyber security events related to maritime from the last decade.
- A prioritized list of the top-10 cyber threats based on previous incidents.
- A brief discussion of contemporary and future threats.

Figure 1 shows the resulting top-10 cyber threats, which shows that there has been a wide variety of attacks. In general, there has not been a large number of incidents compared to other sectors, but the consequences of these events have been among the most severe in any sector [3]. Such attacks with low frequency and high impact represent risks that are hard to predict and defend against.

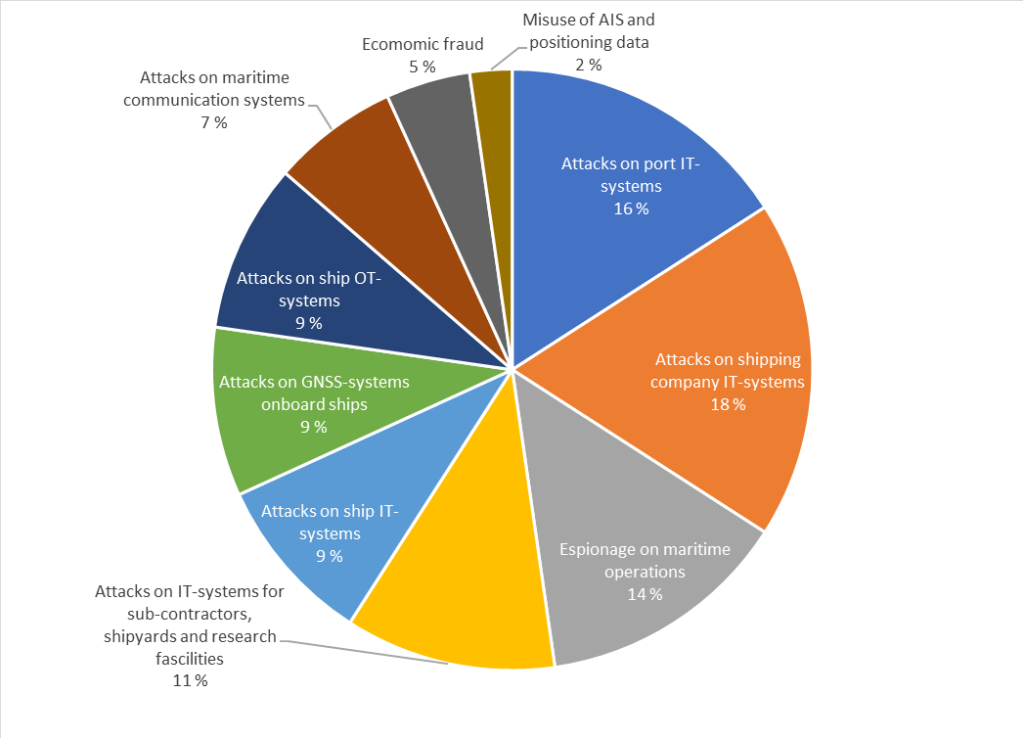


Figure 1. Top-10 cyber threats based on past incidents.

In CySiMS-SE we expanded the maritime incident and threat study in [3] and created a scientific paper for international dissemination. The authors' manuscript of this paper is included in Appendix A.

As an additional input to the Maritime Strategy for Digital Security [4] developed in collaboration by the Norwegian Maritime Authority and the Coastal Administration, DNV-GL [5] conducted an online survey among stakeholders in the maritime industry regarding vulnerabilities. From this study, 51 respondents indicated that the most vulnerable systems were:

- Software-based control and automation systems onboard (62,7%)
- Software-based navigation and communication systems onboard (52,9%)
- Software-based information systems onboard (33,3%)
- Other systems onboard (11,8%)

The survey also showed that IT-systems onshore are standard *commercial off-the-shelf* (COTS) products and share the same risks as in other sectors.

The CySiMS-SE PKI is basically a distributed system that resides on-shore as a part of IT-systems, communication system and tied to OT/navigation and IT-system onboard. Hence, there are many different attack entry points that can have an impact on the operations and services relying on the PKI.

3 Risk estimation

As already mentioned in the previous section, attacks with low frequency and high impact represent risks that are hard to predict and defend against. This is because past incidents cannot really give a good idea of the risks for new designs in an evolving threat landscape. We also saw in the previous section that attackers have been using a variety of attack entry points and methods.

Our extended risk methodology takes such concerns into account and look at various threats that can lead to unwanted events, and different consequences that could follow them. The threat estimations are based on the availability of potential threat actors, their opportunities of performing attacks, the required means (resources) that are needed for the attack to succeed, and motivation factors. Such estimations are less

dependent on historical events data, and are therefore allow us to use a proactive approach for assessing the risk of new designs and prototypes.

Figure 2 shows the steps we have been using for expanding our methodology for risk estimation. We initially developed the risk methodology itself for our purpose. It is based on existing approaches, such as bow-tie modelling closely linked to *formal safety assessment* (FSA), capability-based modelling in the form of resource cost trees and determining attack paths using the cyber kill chain. These techniques are explained in detail in D2.1 [2]. The methodology was validated using system owners for parts of business case 1, specifically the ECDIS connected to a NavStation and the bridge communication system. The validation study allowed us to create generic threat modelling templates as we saw the resource costs trees shared so many common elements. This allowed us to more efficiently model unwanted events for other situations in the business use cases. The combined results are used to evaluate and compare the risk values of the various unwanted events, and ultimately support decisions on security investments.

Figure 2. Steps for the updated risk estimation.

Central to the methodology is the identification of unwanted events, threats that can lead to such events, and potential consequences. The section below contains an explanation how we have identified these based on the methodology in D2.1 [2].

3.1 Unwanted event and threats

Our analysis of the cyberthreat landscape in Appendix A showed that malware infection is the prevalent way of compromising systems, and we have therefore focused the scope of our analysis towards these types of threats. The unwanted event is related to malware compromise towards different systems or components used in the context of the PKI and the operational pilot as described in “D1.2 Evaluation of the operational pilot” [6]. Figure 3 shows three of the threats linked to attack points for shore-based systems and Figure 4 the same for onboard systems.

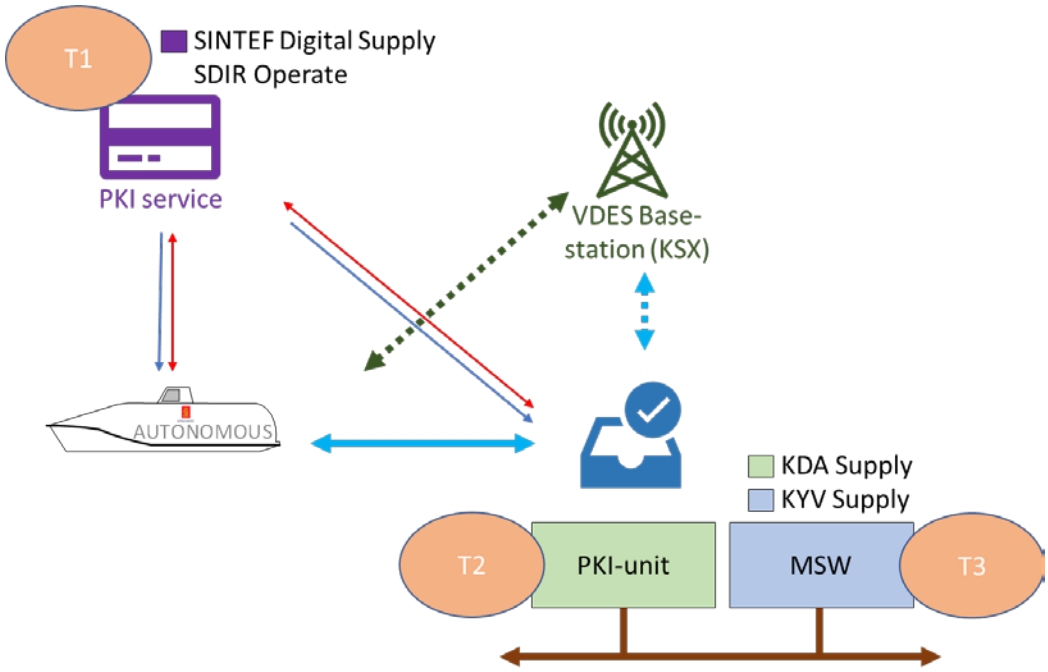


Figure 3. Threats targeting shore-based systems related to the PKI.

The PKI service is responsible for receiving certificate signing requests, issuing certificates and revoking certificates. The software is supplied by SINTEF Digital based on the OpenXPKI project and operated by the Norwegian Maritime Authority (SDIR). The Maritime Single Windows (MSW) is supplied and operated by the Norwegian Coastal Administration (KYV), and relies on a local PKI-unit, supplied by Kongsberg Defence and Aerospace (KDA), for verifying and signing messages from ships.

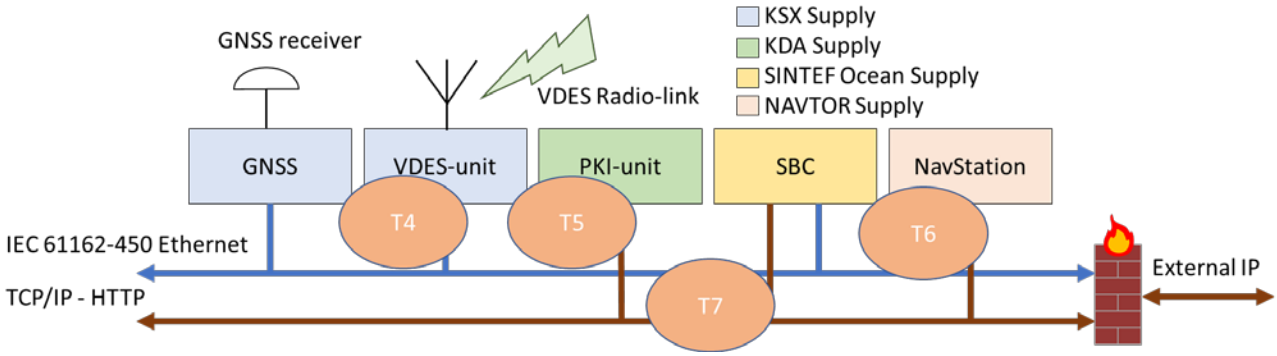


Figure 4. Threats targeting onboard systems related to the PKI.

Onboard the ship there are a number of reference systems/components that are relevant for the business cases. The VDES-unit, supplied by Kongsberg Seatex (KSX), is used to communicate to other surrounding ships and the MSW. The PKI-unit is equal to the one onshore, but operates in a different environment and has a different threat picture. The NavStation is an integrated voyage planning and electronic chart management station supplied by NAVTOR that uses the PKI-unit for securing messages. The Bridge communication system provides the communication infrastructure between the systems/components. The Single Board Computer (SBC), provided by SINTEF Ocean, is only used for test purposes in the operational pilot, and hence not part of the risk assessment scope. The Global Navigation Satellite System (GNSS) is also outside the scope of the risk assessment, though it provides data that is central to the NavStation.

The figures above contain the following threats where malware is the reason for compromise:

- T1: PKI service compromised at operator (SDIR/SINTEF Digital)
- T2: PKI-unit used by MSW compromised (KDA/KYV)
- T3: MSW system compromised (KYV)
- T4: VDES-unit onboard ship compromised (KSX)
- T5: PKI-unit onboard ship compromised (KDA)
- T6: NavStation onboard ship compromised (NAVTOR)
- T7: Bridge communication system compromised (SINTEF Ocean)

The stakeholders in parentheses of T1-T7 are the ones best suited for making threat estimations due to knowledge of the system/component.

Figure 5 shows a high-level bow-tie diagram for the unwanted event "Business case compromised". The indicator values for both threats and consequences are intentionally left blank, as the detailed values from the risk assessment are kept internal to the project partners.

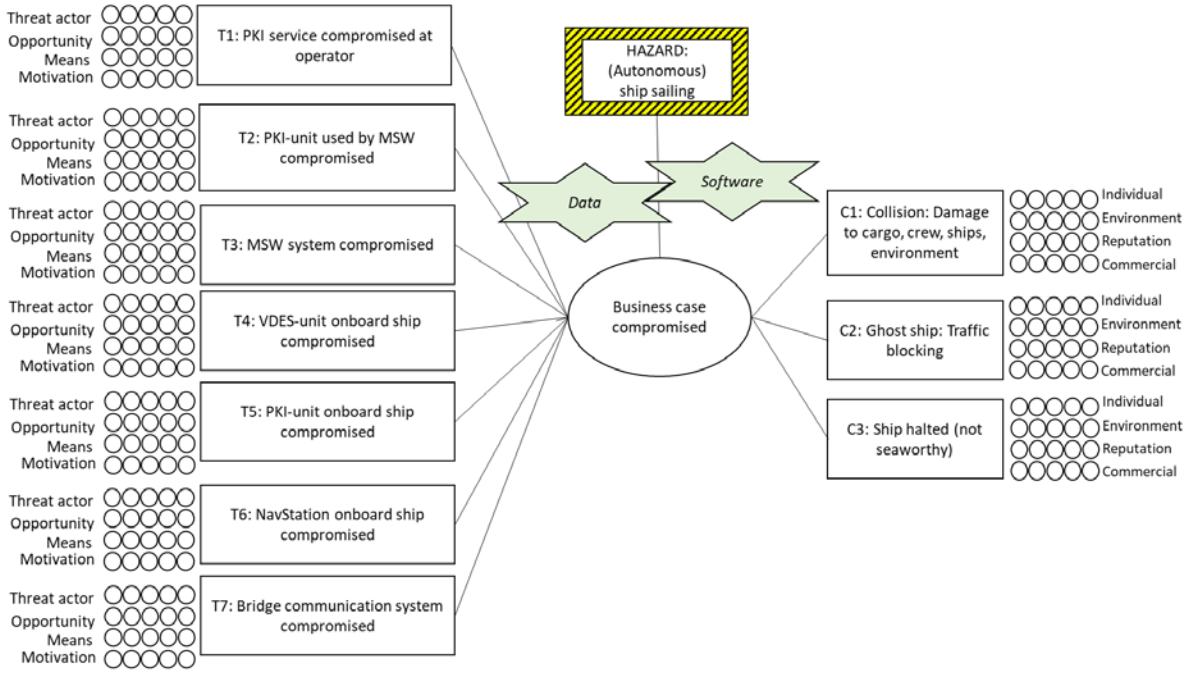


Figure 5. A bow-tie diagram for the unwanted event "Business case compromised".

4 Threat template

We have created a threat template in the form of Excel spreadsheets to estimate values more efficiently for each threat in the bow-tie diagram. The contents are based on the methodology described in D2.1 [2].We have to assume that all threats are possible, but we want to make sure that they are relatively difficult and expensive to realize that we can tolerate the risk.

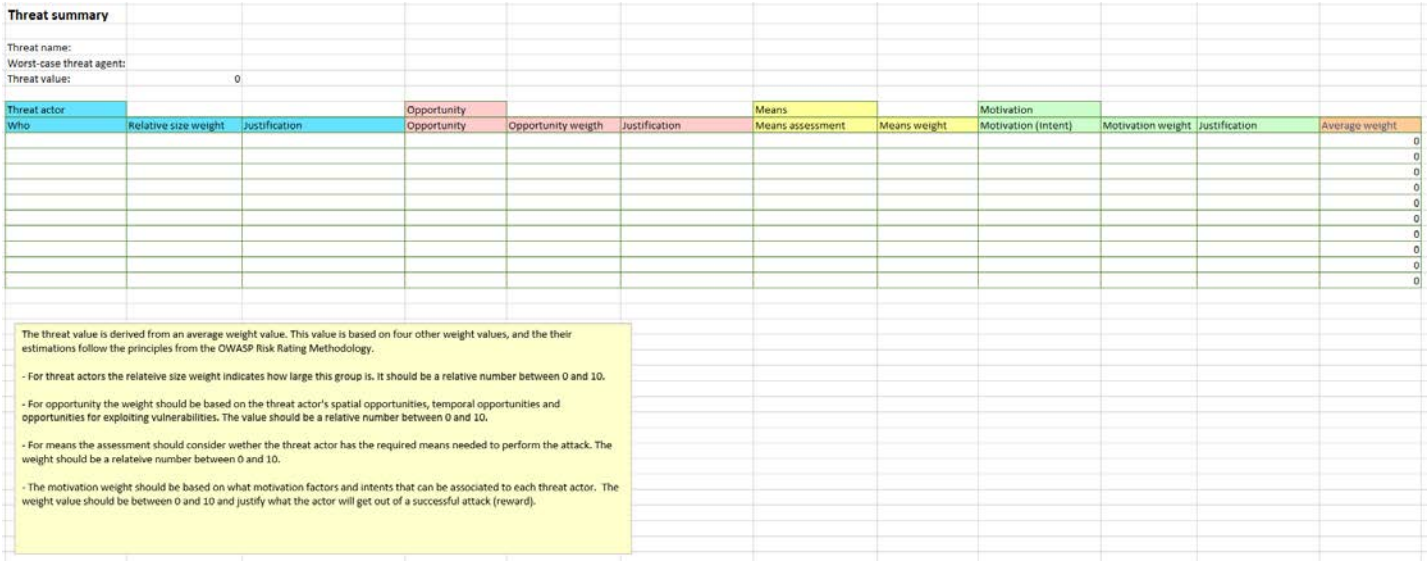
Using the threat template is an iterative approach, where threat actors, opportunity, means, and motivations are identified and given weighted values. This weighted value and the associated threat agent can then be put back into the bow-tie diagram in Figure 5.

Figure 6. The components of the threat template.

Figure 6 gives an overview of the components of the threat template. The treat summary is explained in Section 4.1, threat actors in Section 4.2, opportunities in Section 4.3, means in Section 4.4 and motivation in Section 4.5.

4.1 Threat summary

The threat value summary sheet is shown in Figure 6 and is used to calculate the weights. It takes input from four other sheets, namely threat actors, opportunity, means and motivation.



Threat summary

Threat name:
Worst-case threat agent:
Threat value: 0

Threat actor			Opportunity			Means		Motivation			
Who	Relative size weight	Justification	Opportunity	Opportunity weigth	Justification	Means assessment	Means weight	Motivation (Intent)	Motivation weight	Justification	Average weight
											0
											0
											0
											0
											0
											0
											0
											0
											0
											0

The threat value is derived from an average weight value. This value is based on four other weight values, and the their estimations follow the principles from the OWASP Risk Rating Methodology.

- For threat actors the relateive size weight indicates how large this group is. It should be a relative number between 0 and 10.

- For opportunity the weight should be based on the threat actor's spatial opportunities, temporal opportunities and opportunities for exploiting vulnerabilities. The value should be a relative number between 0 and 10.

- For means the assessment should consider wether the threat actor has the required means needed to perform the attack. The weight should be a relateive number between 0 and 10.

- The motivation weight should be based on what motivation factors and intents that can be associated to each threat actor. The weight value should be between 0 and 10 and justify what the actor will get out of a successful attack (reward).

Figure 7. Threat value summary sheet.

4.2 Threat actors

Figure 7 shows an excerpt from the treat actor sheet.

Threat actor

Threat agents should be defined on the domain. In this case, we have identified potential threat agents from maritime operations, in addition to generic threat profiles. These tables are not meant to be exhaustive, but can be used as inspiration for the threat summary.

Onboard the ship

Title	Description
Captain (aka "master")	Highest responsible officer, represents the ship's owner.
Chief officer/mate	Second in command, mainly responsible for cargo operations. Also responsible for safety and security.
Second officer/mate	Primary duty is navigational and safe passage.
Third officer/mate	Junior to the second mate, primary duty related to safety.
Electro-technical officer	In charge of all the electrical systems on the ship.
Chief Engineer	Responsible for machinery onboard the ship.
Sailor/rating	Performs various duties onboard the ship. May have physical access to the bridge for cleaning duties.
Passenger	Has physical presence onboard the ship but no responsibilities.

At the port/dock

Title	Description
Port Facility Security Officer (PFSO)	Responsible for port security, including access control, surveillance, inspection and handling of cargo.
Clerk	Has general office tasks. When cargo is unloaded from a ship, a clerk checks the actual count of the goods.
IT-administrator	Manages IT infrastructure.
Longshoremen	Dock workers who load and unload ships, or perform administrative tasks associated with the loading or unloading of cargo.
Customs broker	Performs duties related to documentation, cargo clearance, coordination of inland and ocean transportation, dockside inspection of cargo.

Within the shipping company

Title	Description
Chief Executive Officer (CEO)	Makes major corporate decisions and manages operations and resources of the company.
IT-administrator	Manages IT infrastructure.
Company Security Officer (CSO)	Works alongside the ship chief officer/security officer for security purposes.
Clerk	Has general office tasks.
Shipping coordinator	Responsible for export logistics, the execution of shipping services and compliance documentation activities required for in/outbound shipping activities.

Figure 8. Threat actor suggestions.

4.3 Opportunity

Figure 8 shows the template sheet for determining opportunities tied to the phases of the cyber kill chain. Input to the columns when, where and vulnerability can be based on Figure 9, Figure 10 and Figure 11.

Opportunity

Opportunity can be defined as the presence of a favourable combination of circumstances that makes an action possible. Opportunity can therefore be used as an indicator for when and where, and to some extent how, the threat can manifest itself.

Phase	Where	When	Vulnearbility
Reconnaissance			
Weaponization			
Delivery			
Exploitation			
Installation			
Command and Control			
Act on Objective			

Figure 9. Table for describing opportunities.

As ships have a changing operational environment, we can divide opportunity into several dimensions. The first dimension is the spatial dimension, which is another name for location.

Where	Description
Anywhere	The opportunity is independent of the physical location, meaning that the vulnerability exposure is stable.
Open sea	The attack opportunity is first and foremost present when the ship/rig is on the open sea, isolated from a surrounding infrastructure. Satellite is typically the primary communication channel. There may be other ships in the vicinity.
Close to/along shore	The ship is in the vicinity of a land-based infrastructure, for instance Wi-Fi/cell phone range. It is possible for a threat agent to get physically close to the ship, or even embark it.
Congested waters	The ship is almost constantly close to other ships, but not necessarily close to shore. Peer-to-peer communication is possible.
At dock	The ship is physically connected to a dock/harbour. Perimeter security may or may not be available.
River	The ship is sailing up or down a river, similar to “Close to/along shore”.
Land	The attack opportunity resides within a land-based location, such as the HQ of the shipping company, the VTS center, the dock operations, etc.

Figure 10. Spatial dimension.

The next opportunity dimension is related to time, and we have exemplified these temporal characteristics below. In many cases, the spatial and temporal characteristics will be interlinked, for instance sailing on autopilot is usually performed at open sea, while tugging usually takes place in congested waters. It is possible to have several temporal characteristics for opportunity. For instance, an attack opportunity arises while the ship is sailing on autopilot but would need at least 10 minutes (window size) to succeed.

When	Description
Anytime	The opportunity is independent of time.
Sailing on autopilot	There is an opportunity when the ship is sailing on autopilot.
Manual sailing	There is an opportunity when the ship is sailed by a human.
During operations	There is an opportunity during operations at sea, for instance during fishing, drilling, seismic survey, with passengers onboard, etc.
During inspection	There is an opportunity during ship inspection, which can happen at various physical locations (spatial dimension, e.g. close to shore, at dock).
Tugging	There is an opportunity when the ship is tugged (controlled by another boat).
Unloading/loading	The opportunity arises during unloading/loading operations, which is characterised by the ship standing still and invoking loading systems.
Maintenance	The opportunity arises when there is maintenance work being done to the ship. This could mean that additional people are onboard the ship or they have remote access to the systems.
Daytime/night-time	The opportunity arises at a particular time of the day, for instance during night-time when there are fewer people present on the bridge.
Updating data/software	There is an opportunity during scheduled or unscheduled data/software updates, for instance weekly chart updates.
Reporting	There is an opportunity when the ship is sending reports to shore.
Window size	The vulnerability needs a specific window size to be present, which can be measured in milliseconds, seconds, minutes, hours, days, weeks, months or years. For instance, an attack would need at least 10 minutes to possibly succeed.

Figure 11. Temporal dimension.

The third opportunity dimension that we operate with is related to system vulnerabilities. There must be such vulnerabilities present in order to exploit the system, and we are looking at indicators for this below. Note that many of these indicators are mostly related to legacy systems, and to a lesser degree, new systems still under design/implementation.

What	Description
Age of system/component	Time since the hardware system/component was installed on the ship.
Age of software/updates	Age of the software components or last update/patch.
Know vulnerabilities	System components with known vulnerabilities, such as computers running with the Windows XP Operating System, which is no longer patched against vulnerabilities.
Time since last update	Time since the last software update (that was installed).
Number of components	Find out how many computers or devices are part of the target system.
Network segregation	Determine the system is segregated from other system, either logically or physically.
Uncertified system components	Determine if there are uncertified components of the system that can be used as an entry point.
External interface	Find out which interfaces connects the system to the environment. For instance, bridge network interface, USB syncing devices, direct SatLink connection.
System protection and antivirus software	Presence of dedicated security software and/or hardware controls, such as IDS, firewalls, antivirus, packet inspection, etc.

Figure 12. Vulnerability opportunities.

4.4 Means

The means template sheet is an alternative to the Interactive Resource Cost Model (IRCM) tool described in D2.1 [2] and Haga et al. [7]. Instead of having to model the resource trees from scratch, a generic setup is pre-made and only needs cost values and optionally confidence. The values are calculated for each resource, for each phase and for the total attack. When resource alternatives or phases are irrelevant, the cost cells can be left blank. Templates for each phase of the cyber kill chain are shown in Figure 12, Figure 13, Figure 14, Figure 15, Figure 16, Figure 17 and Figure 18.

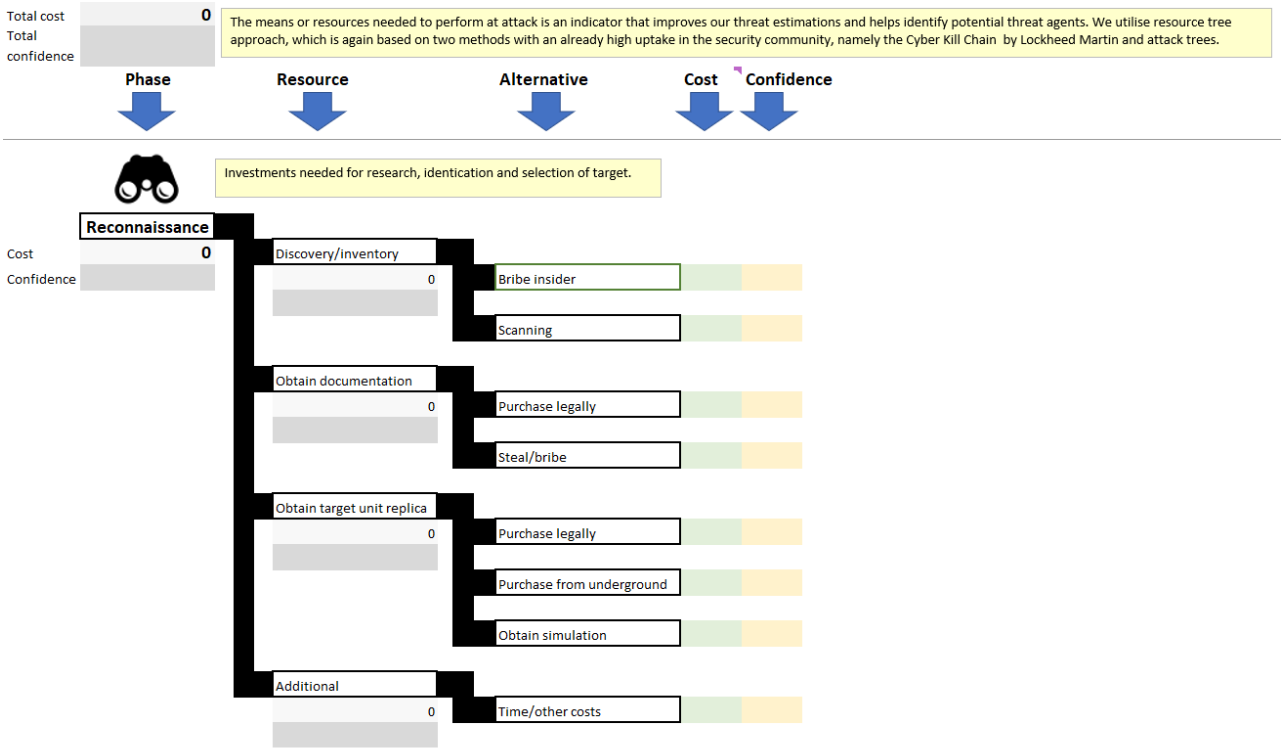


Figure 13. Template for reconnaissance.

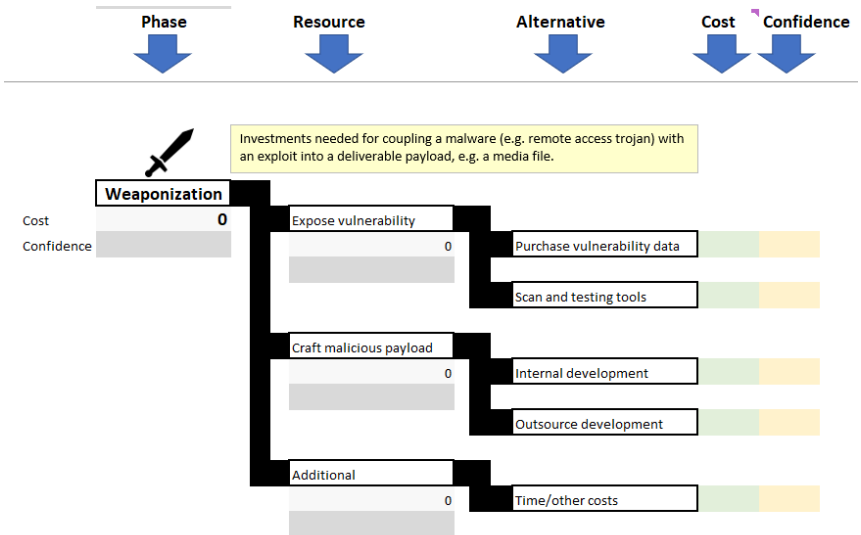


Figure 14. Template for weaponization.

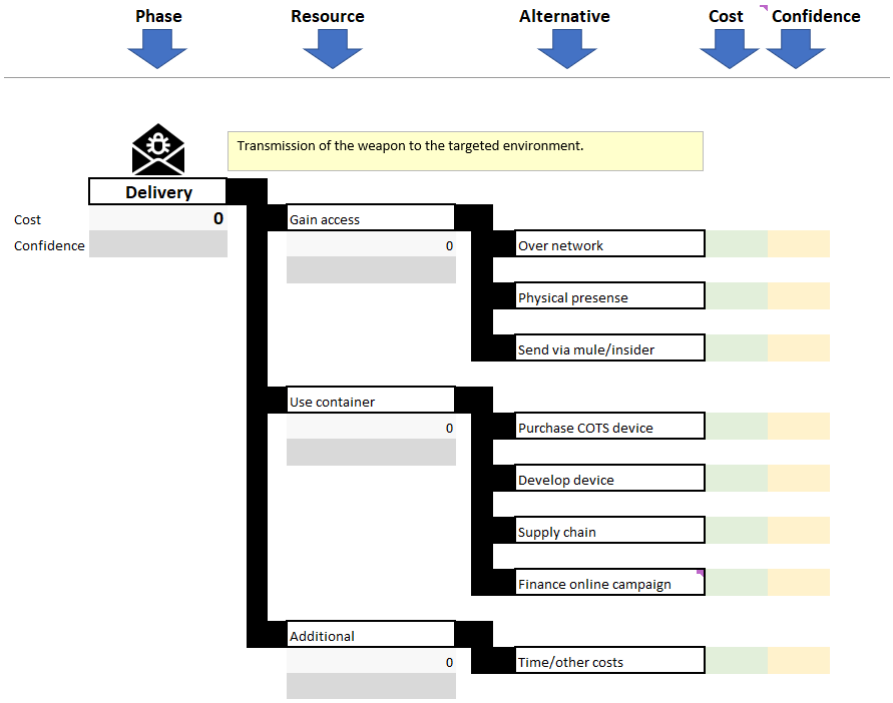


Figure 15. Template for delivery.

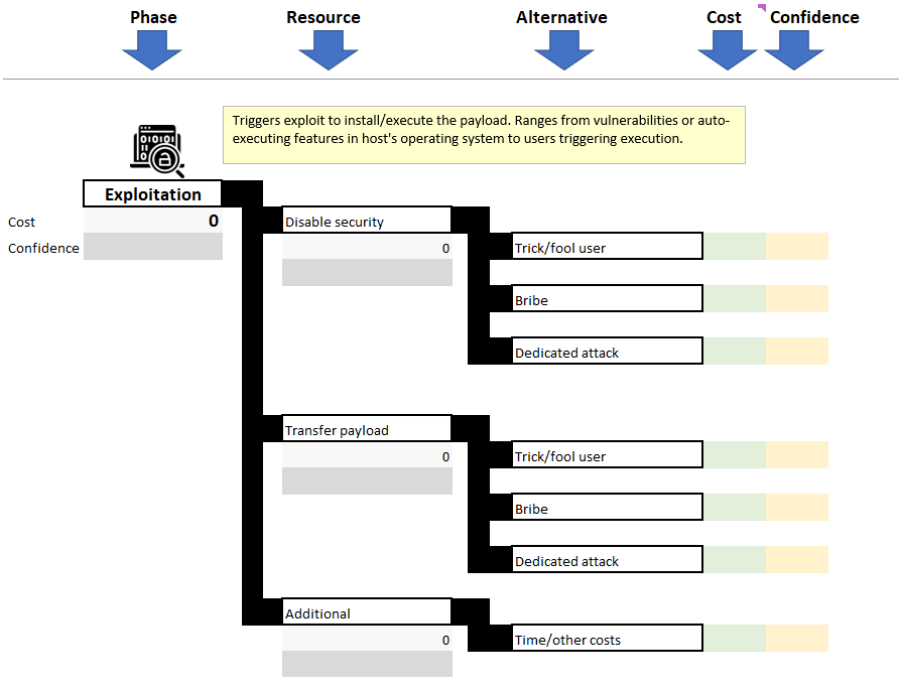


Figure 16. Template for exploitation.

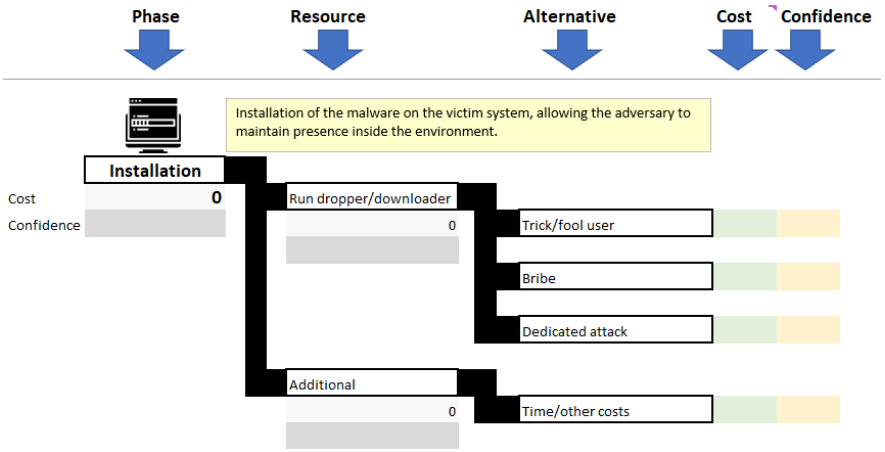


Figure 17. Template for installation.

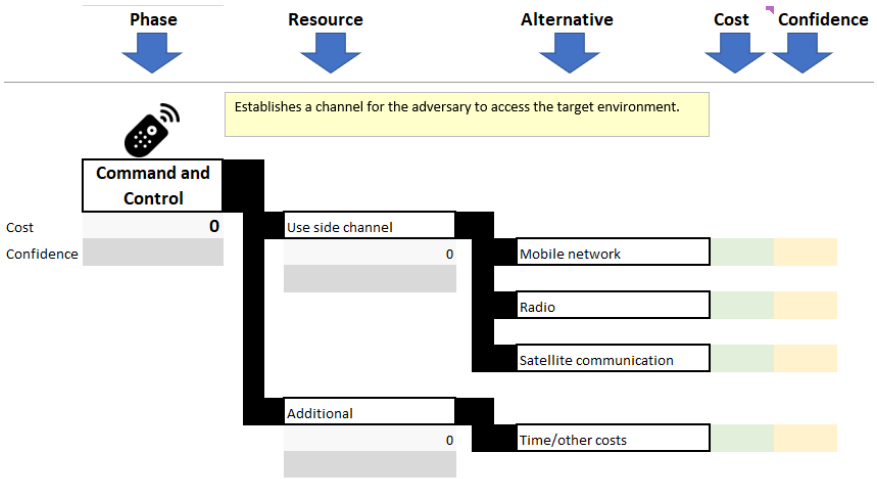


Figure 18. Template for Command and Control.

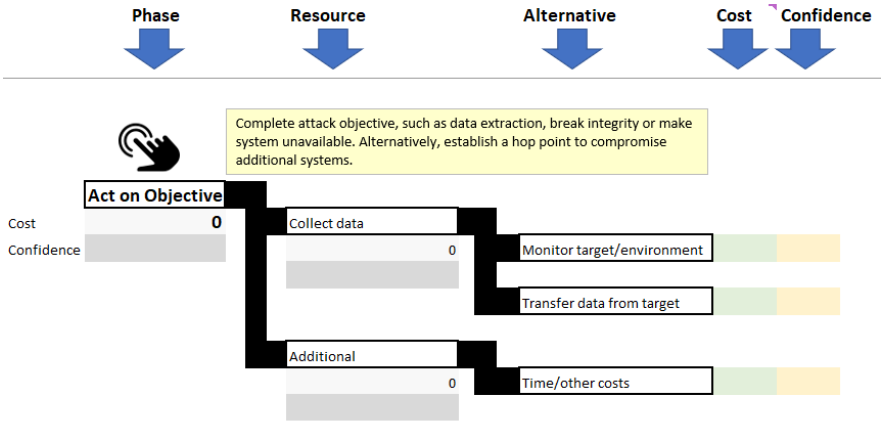


Figure 19. Template for Act on Objective.

4.5 Motivation

The motivation sheet contains motivation elements and intents that can be used as input to the threat summary. Figure 19 and Figure 20 show such suggestions.

Motivation

Motivation identifies the driver that causes the threat agent to commit harmful acts, which again helps identify the nature of the expected harmful actions.

A concept related to motive is intent, which in criminal law is concerned with the purposeful action the threat agent is willing to carry out

Motivation element	Description
Accidental	Benevolent or harmless intent but with actions that inadvertently cause harm.
Coercion	Forced to act illegally on behalf of another.
Disgruntlement	A desire to avenge perceived wrongs through harm.
Dominance	Attempting to assert superiority over another.
Ideology	A passion to express a set of ideas, beliefs, and values that shapes and drives harmful acts.
Notoriety	Seeking to become well known for harmful activity.
Organisational gain	Seeking an advantage of a competitor's organisation.
Personal financial gain	Improve one's own financial status.
Personal satisfaction	Fulfilling an emotional self-interest.
Unpredictable	Acting without identifiable reason or purpose and creating unpredictable events.

Figure 20. Motivation elements.

Intent	Description
Copy	Making an unauthorised copy of an information element. This could for instance be a list of passengers onboard a ship, which could be a confidentiality and privacy breach.
Deny	Making an asset or process unavailable. For instance, a ransomware attack could encrypt the file system of a device so that it cannot be used or accessed. One could also alter access rights of users so that they are locked out of the system or flood the network so that communication ceases to work.
Destroy	Deleting assets (e.g. information or software) or physically breaking a component so that it cannot be recovered.
Damage	Changes to a system that adversely affects is current or future performance. For instance, making a rudder run slower than required could cause navigational mishaps.
Manipulate	Adversely changing information or the behaviour of a system.
Divert	Draw attention away from the real threat or action. For instance, create a distracting event that would take most of the crew's attention, possibly causing strain and lack of resources.
Deceive	Fool the target into thinking that something else is happening. This can be done during the attack or after. For instance, associate fake IP addresses to a network attack so that an innocent party gets the blame.
Control	Take full or partial operational control over a system. For instance, remotely navigate a ship or utilise a component to attack another part of the system.
Take	A form of theft that removes the original asset. For instance, transferring the content of a disk or stealing a bitcoin.
Expose	Give an asset unwanted exposure. For instance, removing the encryption of a communication channel or publishing a confidential document.
Hide	Hide information or code, for instance removing traces of an attack or making installed malware invisible to scanning tools.
Unknown	It is not possible to understand the intentions of the threat actor.

Figure 21. Motivation based on intent.

5 Conclusion

This report provides our assessment of the maritime cyber threat landscape based on past incidents, and shows how to estimate risk for a new design such as the technology related to the CySiMS PKI. The detailed results of the specific analysis are kept internal to the project participants, while we provide the generic templates that have been developed and used for this purpose. These can be further developed, for instance with inclusion of reference values for cost estimates, and applied to other systems with similar context characterisations.

6 References

[1] D. A. Nesheim, Ø. Rødseth, K. Bernsmed, C. Frøystad, and P. H. Meland, "D1.1 Risk Model and Analysis," SINTEF, http://cysims.no/, 2017.

[2] P. H. Meland and K. Bernsmed, "D2.1 Expanded risk and CBA methodology," SINTEF, CYSiMS-SE, 2020.

[3] P. H. Meland, K. Bernsmed, Ø. J. Rødseth, and D. A. Nesheim, "Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet," SINTEF, Jan 15 2020. [Online]. Available: https://www.sdir.no/contentassets/174739a55adb44098b05bcb8ef3b2f65/trusselvurdering-i-forbindelse-med-strategi-for-maritim-digital-sikkerhet-v1_2.pdf?t=1615969701283

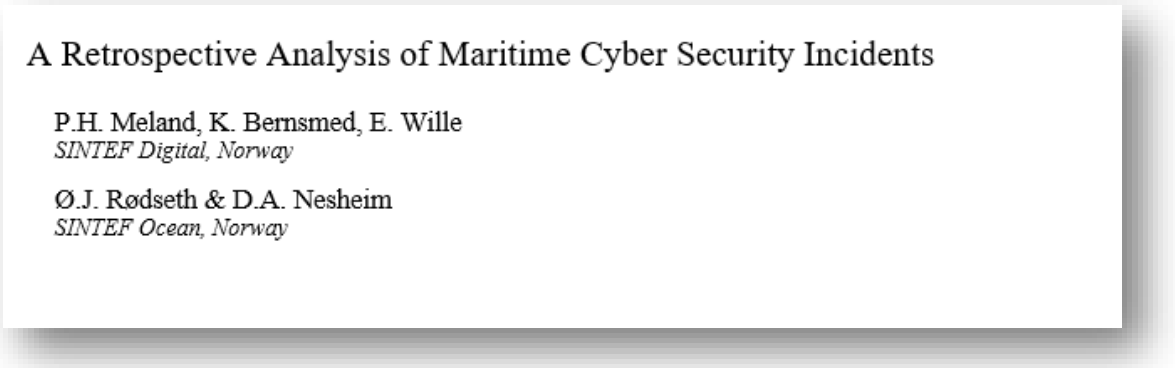
[4] N. H. Bua *et al.*, "Overordnet strategi for maritim digital sikkerhet," Sjøfartsdirektoratet, 2020. [Online]. Available: https://www.sdir.no/contentassets/174739a55adb44098b05bcb8ef3b2f65/2020-12-18---rapport-overordnet-strategi-for-maritim-digital-sikkerhet---v3-klar-til-levering-nfd-og-sd.pdf?t=1615969701283

[5] J. C. Blomhoff, "Sårbarhetsanalyse forbindelse med strategi for maritim digital sikkerhet," DNV-GL, 2020-0927, 2020. [Online]. Available: https://www.sdir.no/contentassets/174739a55adb44098b05bcb8ef3b2f65/dnv-gl---2020-09-15-ros-analyse-for-maritim-digital-sikkerhet-v1---report.pdf?t=1615969701283

[6] Ø. J. Rødseth, K. Bernsmed, P. H. Meland, G. Bour, and D. A. Nesheim, "D1.2 Evaluation of the operational pilot," SINTEF, CySiMS-SE, 2021.

[7] K. Haga, P. H. Meland, and G. Sindre, "Breaking the cyber kill chain by modelling resource costs," in *International Workshop on Graphical Models for Security*, 2020: Springer, pp. 111-126.

A Appendix


A Retrospective Analysis of Maritime Cyber Security Incidents

P.H. Meland, K. Bernsmed, E. Wille
SINTEF Digital, Norway

Ø.J. Rødseth & D.A. Nesheim
SINTEF Ocean, Norway

The manuscript will be included in this report once it has been accepted for publication.