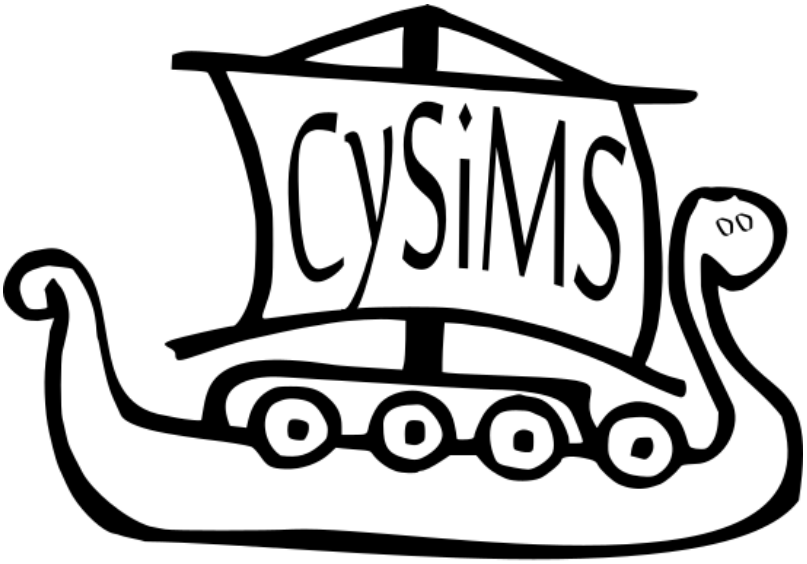
SINTEF

2020:00587- Unrestricted

Report

D2.1 Expanded risk and CBA methodology

Author(s)
Per Håkon Meland
Karin Bernsmed



SINTEF Digital
Cyber Security
2020-06-25

SINTEF Digital
SINTEF Digital
Address:

NO-
NORWAY
Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

Report

D2.1 Expanded risk and CBA methodology

KEYWORDS:
Cyber security, maritime, PKI, VDES, risk assessment, bow-tie, cost-benefit analysis

VERSION	DATE
1.0	2020-06-25

AUTHOR(S)
Per Håkon Meland
Karin Bernsmed

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

PROJECT NO.	NUMBER OF PAGES/APPENDICES:
102019295	44

ABSTRACT

The goal of the CySiMS SE solution is to prove economical as well as security and safety benefits. This needs to be quantified and documented in a systematic way. The risk assessment methodology developed in CySiMS has been extended with ways to obtain input values needed to perform accurate assessments when there is no or little statistical data available. We have further developed it into a more complete Cost-Benefit Analysis (CBA) tool that can support security decision making.

PREPARED BY	SIGNATURE
Karin Bernsmed	

CHECKED BY	SIGNATURE
Guillaume Bour	

APPROVED BY	SIGNATURE
Maria Bartnes	

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
2020:00587	978-82-14-06513-8	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2020-06-25	Final version after internal check by Guillaume Bour, peer review by Nils Haktor Bua and project manager approval by Dag Atle Nesheim.

SINTEF

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 a 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 document describes an expanded risk assessment methodology based on the initial work done in CySiMS, which now also allows Cost-Benefit Analysis related to security measures to be made. We have to assume that any system can be compromised, but we can give a reasonable security assurance when there few threat actors capable and willing to perform cyber-attacks.

The risk assessment methodology explained here should consider a specific time period, e.g. a year, before it should be repeated. This assures a credible validity period and a more accurate assessment.

2 Background

In the CySiMS project, two high-level modelling techniques were developed: a threat and risk assessment framework [1], implemented as an Excel-based tool [2], and a methodology for modelling causes and effects of security threats using bow-tie diagrams.

The CySiMS threat and risk assessment framework, documented in [1], presents a framework for identifying and estimating the cyber risk levels of maritime systems and technologies. The framework includes a method for computing risks, based on the likelihood and consequence of unwanted events. The risk levels are measured in a semi-quantitative manner. The impacts are assessed on two levels: 1) the likelihood of the potential consequence of an unwanted event, and 2) the likelihood of the unwanted event itself. The consequence levels are selected from a set of pre-defined areas: 1) individual health or life, 2) societal, 3) economic, 4) reputation and 4) environmental areas. The framework includes suggested levels for acceptable and unacceptable risks and promotes that the target should be as low as reasonably practicable (ALARP). The framework has been implemented as an Excel-based tool [2].

In the CySiMS deliverable D1.1 [1], the framework was applied on 12 different scenarios, for which the risks of communication related threats relevant for the future Maritime Service Portfolio were assessed. Figure 1 provides an example from the tool [2], in which the risk of the scenario " Navigational Real Time Information to Ship " has been assessed.

			Main Threat		Main	Main Impact		
Scenario	Description	Main Asset	Threat	Likelihood	Unwanted Event	Worst Consequence	Impact	Risk
Scenario 1: Navigational Real Time Information to Ship	The ship receives updated navigational information from shore. Examples are weather or ice information and forecast, lists of aids to navigations that are not working, floating containers, whale observations, wrecks etc. Today this is typically maritime safety information (MSI) received by NAVTEX or Safety-Net or wave, tide or virtual aids to navigation received over AIS.	MSI Data	Jamming of terrestrial link	3	Data lost	Not receiving updated information in a short time that could develop in an accident, e.g wreckage at the exit of shallow waters/canals	8	11
Expert Opinion on Security Measures	This threat is difficult to mitigate. However, the impact of the unwanted event can be reduced by introducing procedures and contingency plans for managing such events, as well as establishing alternate means of communication if required							

Figure 1. Risk assessment of the scenario "Navigational real time information to ship".

The CySiMS methodology for modelling causes and effects of security threats using bow-tie diagrams, documented in [3], [4] and [5], is an approach that combines security with bow-tie safety assessment. The methodology is focused on unwanted events, which are represented in the middle of the model (one event per model). The left side of the model includes the threats that may cause the event, and the right side of the model includes the potential impacts of the event. The model also includes preventive and reactive controls.

To help assess likelihood and consequences of the risk level of the unwanted event, we also included a way of assessing the likelihood of the left-hand side threats and the severity levels of the potential impacts on the right-hand side. An example is provided in Figure 2. The methodology has been implemented as an online web-based tool [6].

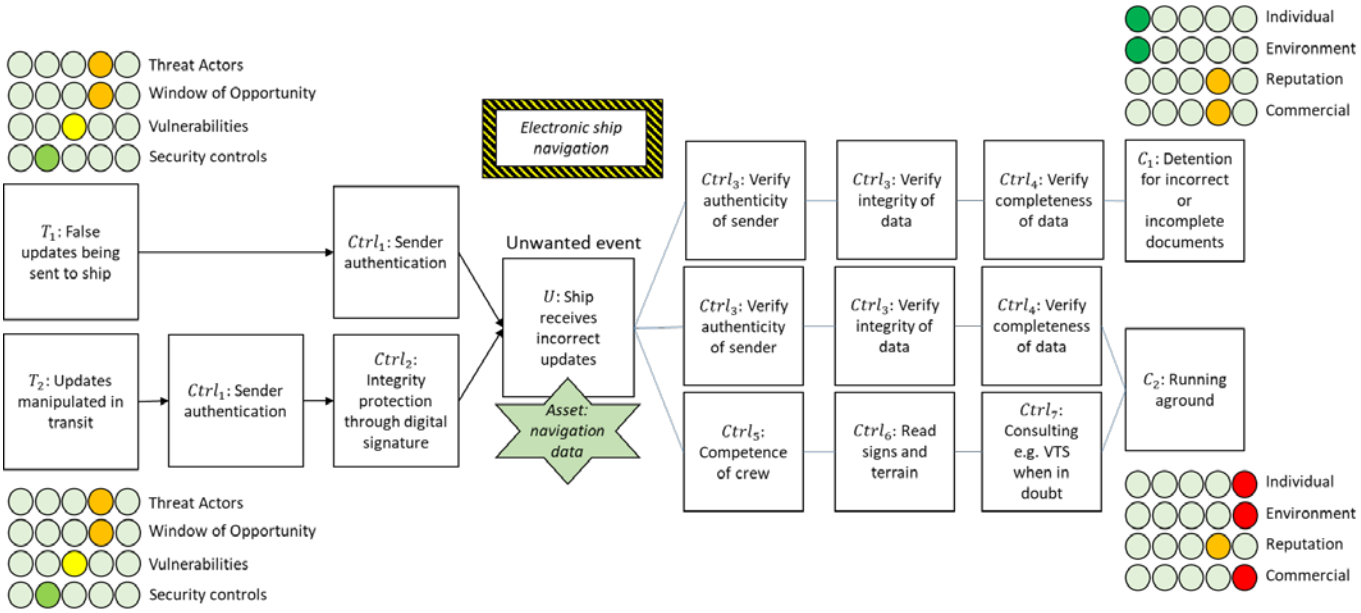


Figure 2 Risk assessment of the unwanted event "Ship receives incorrect updates".

In our method, an unwanted event U will be a function of one or more threats. Each unwanted event will lead to one or more consequences C, where each identified consequence is associated with a corresponding impact (i.e. severity, or loss,) value L. The risk R associated with a certain unwanted event U, which we denote $R(U)$, will then be approximated as the probability that the unwanted event occurs, i.e. $p(U)$, multiplied with the worst-case consequence impact value that has been identified, which we denote L_C, and the likelihood that this consequence occurs, i.e. $p(C)$. The formal expression for this is:

$$R(U) \approx p(U) \times L_C \times p(C)$$

To quantify the risk of an unwanted event, we hence need to assess 1) the probability of the unwanted event (as a function of one or more identified threats) and 2) the impact value and probability of the worst-case consequence of the unwanted event.

While both these modelling techniques have been successfully applied to assess the risks of a number of maritime scenarios in the CySiMS project, they still share some common weaknesses:

- The difficulty to estimate threats. There is a large body of knowledge, data and statistics available for risk assessment when the events that are taken into account are caused by random failures. However, this is not the case for cyber security threats, where the likelihood estimates tend to be based on gut feeling and best guesses.
- The difficulty to assess the effectiveness of security countermeasures. Risk treatment options should be selected based on the outcome of the risk evaluation (see Section 7.3) and the expected cost and benefits for implementing these options. However, while the cost of purchasing and deploying defence mechanisms may be estimated, it is very difficult to know whether these are worthwhile the required investments.
- Handling known unknowns. Not every threat and control can be prescribed, especially for new technology or usage scenarios. We know that unpreceded situations are likely to occur, also known as "known unknowns". Situation complexity and available resources will determine how incidents should be tackled, and there must be room for variations.

These issues will be further investigated in this deliverable.

3 Example

The following example is based on demonstration case 1 described in CySiMS-SE deliverable 1.1. Here, an autonomous ship transmits an AIS message to its surroundings, containing next waypoint, course, speed, heading, ship length, etc. The update frequency of this signal is about every 30 seconds. If there is a sudden change then the signal will be sent immediately. The transmission medium is over VDES, and the data will be plotted on the ECDIS of nearby ships.

We will use this example to show how we can estimate threats (Section 4) and select defence mechanisms (section 5) based on a cost-benefit assessment.

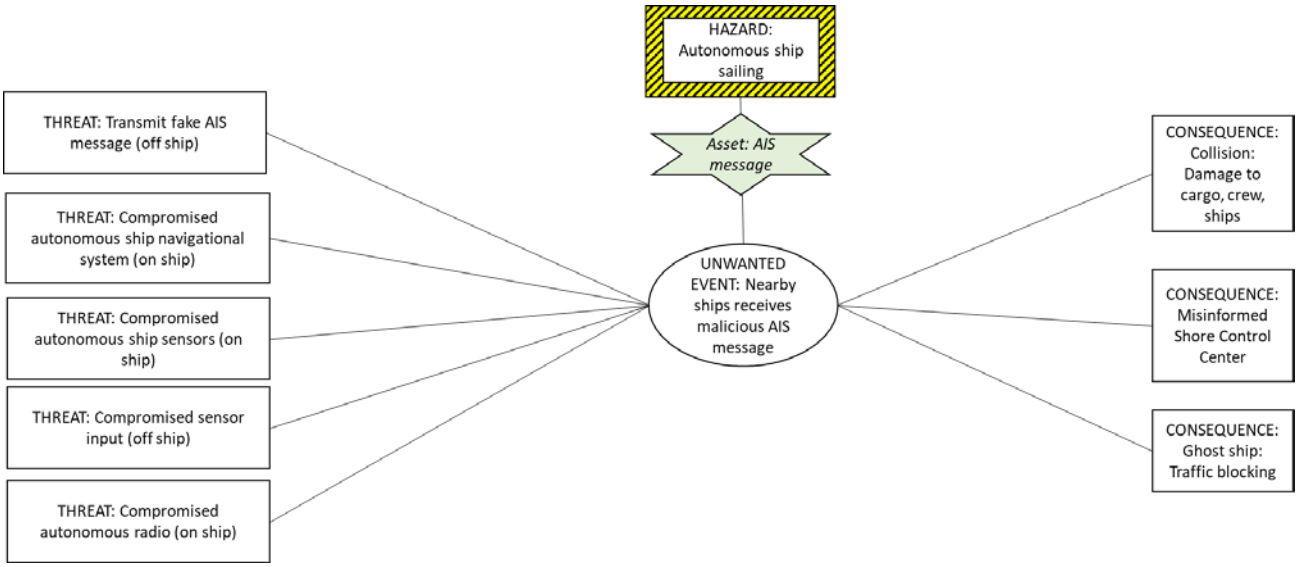


Figure 3. A bow-tie model for the business case 1 example.

Figure 3 shows the high-level bow-tie diagram we would like to assess. Here, the unwanted event is that nearby ships receive a malicious AIS message from the autonomous ship. This can lead to different types of consequences (right side part of the diagram):

- Collision between the autonomous ship and a nearby ship, leading to damage to cargo, crew and the ships themselves.
- Misinformed Shore Control Centre, that would fail to take control over the autonomous ship when needed to.
- Ghost ship appearing on the ECDIS of the other ships, which could block traffic and lead to severe delays in busy ports.

A set of possible causes or threats are shown on the left side part of the same diagram:

- Another ship or an entity off the autonomous ship transmits a fake AIS message. This can be characterised as an impersonation attack.
- The navigational system onboard the autonomous ship is compromised through a cyber-attack and will send out misleading AIS messages.
- Attack towards the sensor system(s) that the autonomous ship depends on for navigation is another threat, for instance false data readings from the thrust control system.
- Compromised sensor input data originating outside the ship can also be a threat, for instance GNSS spoofing from a nearby vessel.
- The radio onboard the autonomous ship could be compromised so that it would change the AIS payload before transmitting it.

4 Improving threat estimation

The following sections provide a threat estimation reference framework tailored for the maritime domain. Using domain-specific knowledge we can create more accurate threat models than if we only consider generic systems and threat agents. However, the level of details should be adjusted to the need of the estimation. One might want to drill down thoroughly for certain threats, which requires more effort than giving a more superficial estimation for threats that are already well-known. For similar threats it might be sufficient to do a detailed analysis of one and use those results for the others.

4.1 Determining threat actors

Every crime has at least one perpetrator and determining potential threat agents is important to create a common threat picture in any domain [7]. Shinder and Tittel [8] define a *profile* to be a set of characteristics likely to be shared by criminals who commit a certain type of crime. The use of profiles during criminal investigations can be traced several hundred years back in time, and though this is not an exact science, Nykodym et al. [9] argue that the track record legitimates the concept. However, they also argue that attackers have more advantages in a cyber setting as they do not have to be physically present at the crime scene.

The two main methods for profiling are known as *inductive* and *deductive* [10]. In the former, a profile database is developed based on information from already committed crime, and offender characteristics are correlated with types of crime. In the latter, forensics evidence is gathered from the crime scene and used to deduce the characteristics of the offender. Most of the established literature comes from the digital forensics field and relates to deductive profiling. We are mostly interested in inductive profiling as a tool to identify potential offenders before any crime is actually committed and establish measures that will prevent such events.

A profile overview established in the CySiMS project is shown in Appendix A. This overview was not meant to be complete, but rather serve to demonstrate that there are several types of actors with the motivation and capability to pose a cyber threat independent of any industry. However, specialisation can be more useful on

a case to case basis in order to make the threat actors as relevant as possible. In this section we show a more specialised sample for the maritime domain ([11]) that can be used as a starting point for inductive profiling.

Table 1 is based on [12] and shows various profiles with physical presence onboard a ship. All of these can be seen as specialisations of a malicious insider profile (Appendix A), but with somewhat different characteristics.

Table 1. 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.

In Table 2, there are possible insiders found at the port/dock [13]. Similarly, Table 3 shows relevant profiles within the shipping company, Table 4 people within the flag state organisation and Table 5 within the Vessel Traffic Services.

Table 2. 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.

Table 3. 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.
Technical worker	Works in land-based office on call to assist autonomous ships across the oceans [14].

Table 4. Within the flag state organisation

Title	Description
Inspector (aka marine surveyor)	A person who conducts inspections, surveys or examinations of marine vessels to assess, monitor and report on their condition and the products on them [15].
IT-administrator	Manages IT infrastructure.
Clerk	Has general office tasks.

Table 5. Within the Vessel Traffic Services

Title	Description
Vessel traffic coordinator/VTS operator	Monitors traffic and periodically makes nearby vessels aware of other vessels, tugs or hazards.
IT-administrator	Manages IT infrastructure.
Clerk	Has general office tasks.

In Table 6 there are various profiles related to application/system providers for both ship and shore. These will normally not have a physical presence but might have remote access or come visit to do maintenance and/or installation tasks.

Table 6. Application/system provider

Title	Description
Chief Executive Officer (CEO)	Makes major corporate decisions and manages operations and resources of the company.
IT-administrator	Manages IT infrastructure.
Clerk	Has general office tasks.
Data processor	The data processor processes personal data only on behalf of the data controller [16].
Maintenance crew	Performs maintenance, replacement or instalments of ship systems. Requires either physical access and presence or remote operations capabilities.

The general profile Activist hacker is described in Appendix A, but could be elaborated further as shown in Table 7.

Table 7. Activist hacker

Title	Description
Environmentalist	Concerned about pollution stemming from the shipping industry. Might want to get hold of confidential data about emissions, fuel consumption, etc.
Species protectionist	Concerned about how shipping routes can endanger animals. Might try to make ships avoid certain areas or track the use of sailing ballast.
Political activist	May try to take a direct and militant action to achieve a political goal.

Table 8. Pirate/criminal shows specialisations of the pirate/criminal profile, where we have tried to highlight the ones that are likely to operate in a maritime setting.

Table 8. Pirate/criminal

Title	Description
Cyber extortionist	Will typically try to seize a digital asset or function and demand payment for its release.
Smuggler	Could for instance try to falsify cargo information in order to smuggle illegal goods such as drugs and firearms.
Fraudster	Can for instance impersonate a business partner and try to get payment for a non-existing service. Commonly uses fake invoices.
Information thief	Looking to steal ship related information that could be misused to e.g. manipulate the stock market or sold to a competitor. Information about vulnerable ships and cargo content could also be used in order to plan a physical robbery. This actor could also be interested in personal information about crew and passengers.

The remaining profiles that can be found in Appendix A are given in Table 9. These can be further specialised for the maritime domain when relevant.

Table 9. Generic threat actors

Title	Description
Government Cyber Warrior	The never halting race for military power and advantage makes governments a highly motivated threat actor. Disrupting the shipping operations of a country or region might serve to demonstrate such capacity and power. In the event of a military conflict, gaining control of the opponent's national fleet might be of strategic importance.
Government Spy	Developing technology is expensive. Some countries use government intelligence services to obtain new technology for their national industry. Governments are also interested in learning more about the people and technologies of businesses for general surveillance purposes.
Script kiddie	Script kiddies utilizes pre-created software and scripts to direct attacks at a target. The script kiddies could be young, aspiring hackers trying to learn the game and make a name for themselves.
Security researcher	Highly skilled individuals might attack the system in order to find new flaws and thus intentionally or unintentionally cause service disruption. They could be motivated by the mental challenge, prospect of fame or the possibility to prove their skills.
Former employee	This is mostly the same as for the malicious insiders if no routine exists for removing access upon leaving the company. If routines for removing access are in place and executed correctly, the perpetrators capability is reduced. The perpetrator will still have extensive knowledge about the systems and their configuration but will have to obtain access through other means than using his own.
Terrorist	Over the last couple of years, terrorist organisations have demonstrated their commitment and high motivation for their cause – although said causes differ.

	Well-known terrorist groups include ISIS, Al Qaeda and Al Shabab, while smaller groups have been targeting ships in the Indian Ocean waters [17].
Competing Shipping Company	Shipping is a competitive industry and some actors might turn to hostile methods in order to increase their profits. Knowing the industry and the systems, they make a noteworthy adversary.

The next step is to try to figure out whom, if any, of these would be capable of realising the threats. Also, it would be interesting to know if there exist many such candidates (e.g. many competitors or passengers) for each threat case. To make such an assessment, we propose a systematic approach based on the established fact that that likely offenders have *opportunity*, *means* and *motive* (MMO) [18, 19] before committing any crime. This is elaborated in the following sections.

4.2 Opportunity

Opportunity can be defined as the presence of a favourable combination of circumstances that makes an action possible [20]. Opportunity can therefore be used as an indicator for *when* and *where*, and to some extent *how*, the threat can manifest itself. The most severe threats can exploit vulnerabilities at anytime from anywhere, while in other cases the adversary must be *at the right time at the right place*. In practice, we have to accept that not all vulnerabilities can be eliminated in order to have reasonable security costs and meaningful operations. However, we should strive to make the *window of opportunity* as small as possible so that the adversary cannot easily attack the system without being noticed.

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. In Table 10 we give examples of such spatial characteristics that can indicate the threat seriousness.

Table 10. Spatial characteristic for opportunity

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.

The next opportunity dimension is related to time, and we have exemplified these temporal characteristics in Table 11. 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.

Table 11. Temporal characteristic for opportunity

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.

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.

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 in Table 12. Note that many of these indicators are mostly related to legacy systems, and to a lesser degree, new systems still under design/implementation.

Table 12. Opportunity for exploiting system vulnerabilities

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.

4.3 Means

The means or resources needed to perform at attack is another indicator that improves our threat estimations and helps identify potential threat agents. We utilise an approach described by Haga et al. [21], which is again based on two methods with an already high uptake in the security community, namely the *Cyber Kill Chain*™ by Lockheed Martin [22] and *attack trees* by Bruce Schneier [23]. Here, a resource tree is modelled for each consecutive stage in a specific type of cyber-attack. These trees estimate the necessary resources that are required to complete this stage and move on to the next one. The tree consists of a root node, defining the cyber kill stage, a second level of conjunctive *resource classes*, and a third level of disjunctive *resource alternatives*. An illustration of this structure is shown in Figure 4.

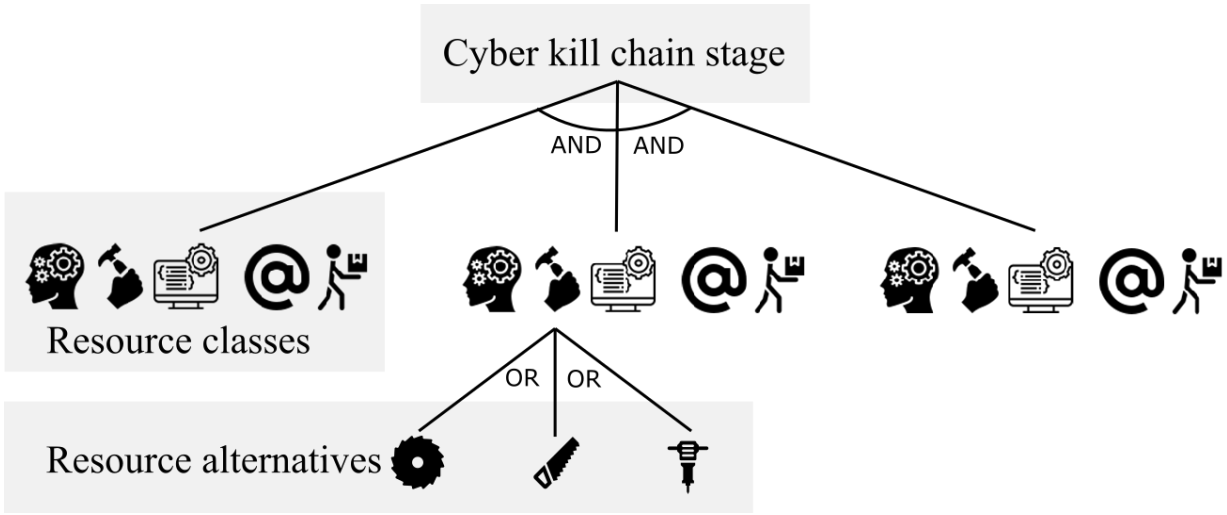


Figure 4. A resource tree example

The cyber kill chain originally has seven stages, namely:

Reconnaissance - Research, identification and selection of target.

Weaponization - Coupling a malware (e.g. remote access trojan) with an exploit into a deliverable payload, e.g. a media file.

Delivery - Transmission of the weapon to the targeted environment, e.g. an email attachment or USB-drive.

Exploitation - Triggers malicious code. Ranges from vulnerabilities or auto-executing features in host's operating system to users triggering execution.

Installation - Installation of the malware on the victim system, allowing the adversary to maintain presence inside the environment.

Command and Control (C2) - Establishes a channel for the adversary to access the target environment.

Actions on Objectives - Complete attack objectives, such as data extraction, break integrity or make system unavailable. Alternatively, establish a hop point to compromise additional systems.

As shown by Pols [24] there are many variants of the kill chain found in the literature. Some with different stage types and others with up to eighteen different stages. We will use the default stages from Lockheed Martin as a reference, but it might be more suitable to use other sets for attacks that are not malware-related, for instance social engineering or denial-of-service.

Resources can be classified according to five different types, namely:

Skill - Includes domain knowledge, malware development abilities or utilisation of cybercrime tools or guides.

Tangible - Necessary hardware components or other physical objects. This can range from advanced technology to soldering tools.

Logic - Commercially available software, data sets or cybercrime tools or services.

Logic-atomic - Necessary resources that cannot be broken into smaller parts, e.g an IP-address, email address or a password.

Behavioral - Actions that must be conducted as a part of the attack, for instance bribing, sending out phishing emails or social engineering.

Each resource class should have at least one alternative with an associated cost range and optional confidence value (between 0 and 1). The approach allows for a calculation of the cheapest and most expensive attack. There is a dedicated tool for this approach, which also allows to identify potential threat agents based on a pre-defined library of cybercriminal profiles. The tool also implements a set of characteristics for each resource alternative that helps limit the set of potential threat agents.

Figure 4 shows an example screenshot from the reconnaissance stage of an attack targeting the ECDIS onboard a ship. This example is inspired by the successful ECDIS attack demonstrated by Lund et al. [25].

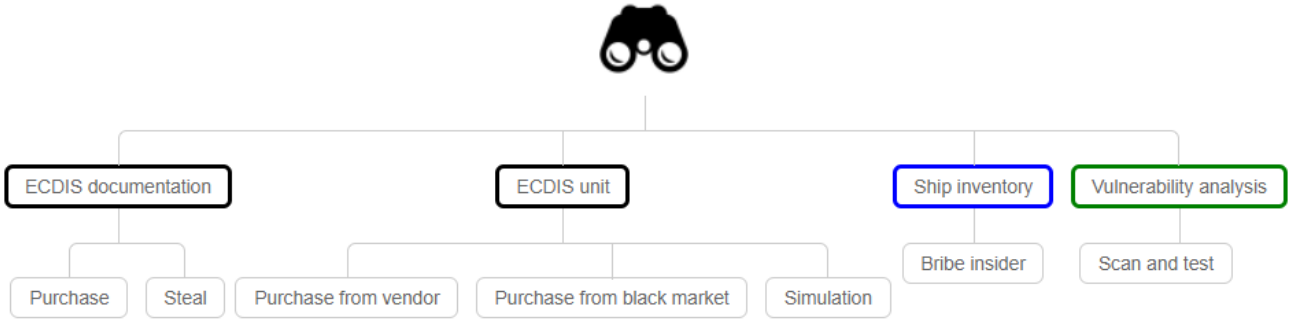


Figure 5. A reconnaissance screen shot example

As can be seen in the figure, there are four resources defined for the reconnaissance stage. The first one, *ECDIS documentation*, is a tangible class, and the alternatives are to either *purchase* the documentation from the vendor legally or *steal* it. The second resource is another tangible class and represents an operational ECDIS unit that can be used to analyse its operating system, software and network traffic. It can be realized in different ways, by *purchasing a unit from vendor* or the *black market* or running it as a software *simulation*. These alternatives vary in price, from relatively cheap software (where you pay according to sailing route) to more expensive hardware units in the range of $10 000 - $30 000. The third resource is of class logic-atomic and represents information about the *ship inventory* used to determine which type and where the ECDIS units are installed. To simplify the model, only a single *bribe insider* alternative is used. The final resource is also of type skill, and represents required knowledge about *vulnerabilities* gained through *scanning and testing*.

Figure 6 and Figure 7 continue showing the complete set of stages for the ECDIS attack example. Here, the cost interval has a broad range [$2876, $85106], mostly due to the choice of purchasing ECDIS hardware unit versus other cheaper alternatives in both the *reconnaissance* and *delivery* stages. Besides from these, the overall resource costs related to tangible and skill are relatively low. By analysing the model, we find that there are significant costs related to the *delivery* stage as the attacker would need physical presence at the ship and gain access to the bridge or bribe an insider. It is the air-gapping of the ECDIS that provides the main security measure by making delivery costly. When considering opening up for online software and chart updates, it is clear that additional secure measures will be needed to preserve an expensive attack vector.

The confidence value is also very low but would have been much higher if we had modelled the attack with a specific ECDIS unit in mind where costs are more certain. Also, a higher number of resources will automatically yield a lower confidence, which is natural since acquiring many resources increases uncertainty. The main benefit of the confidence is for attack comparison, which is not shown in this example.

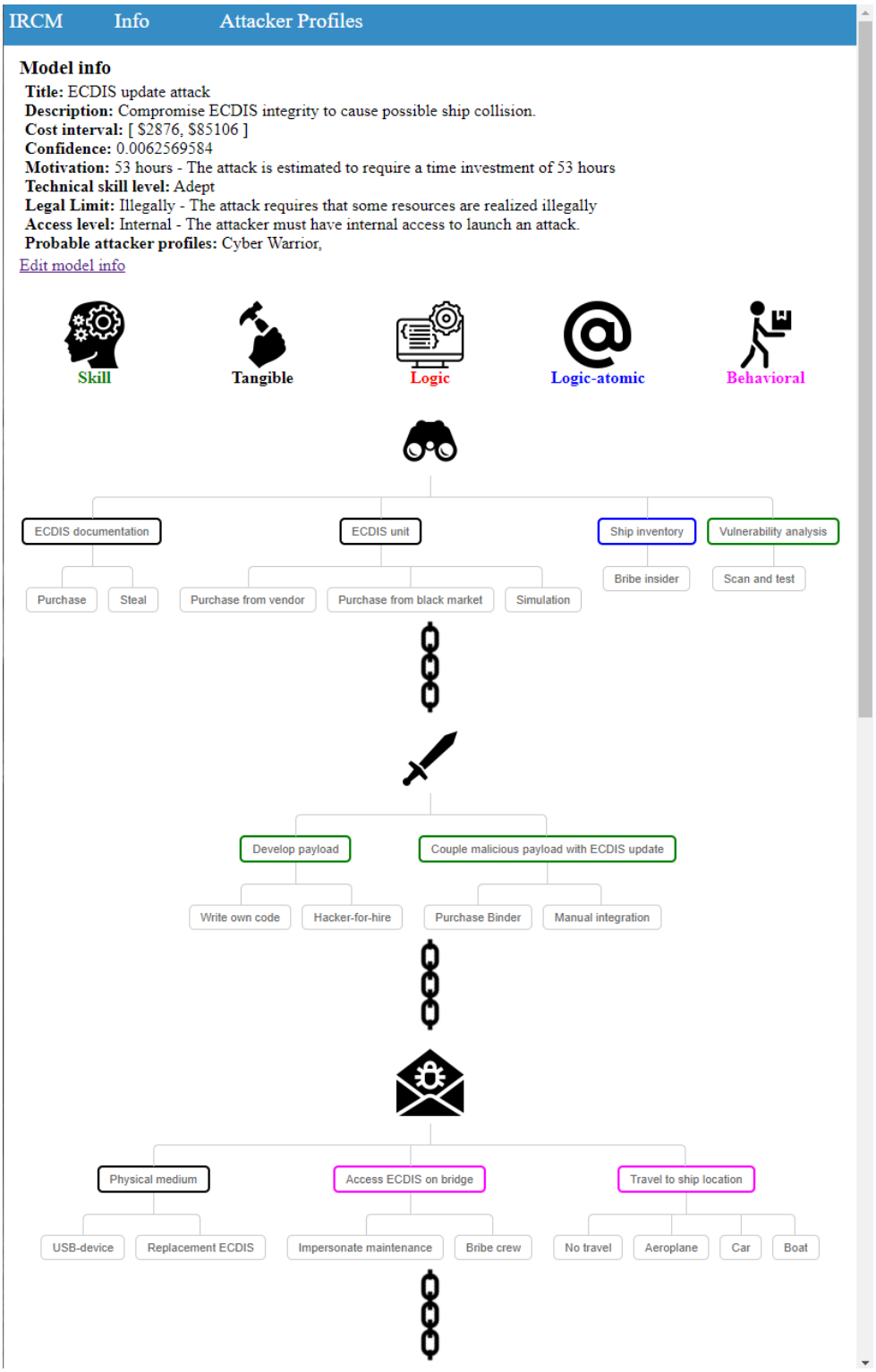


Figure 6. A screenshot from the first three stages; Reconnaissance, Weaponization and Delivery.

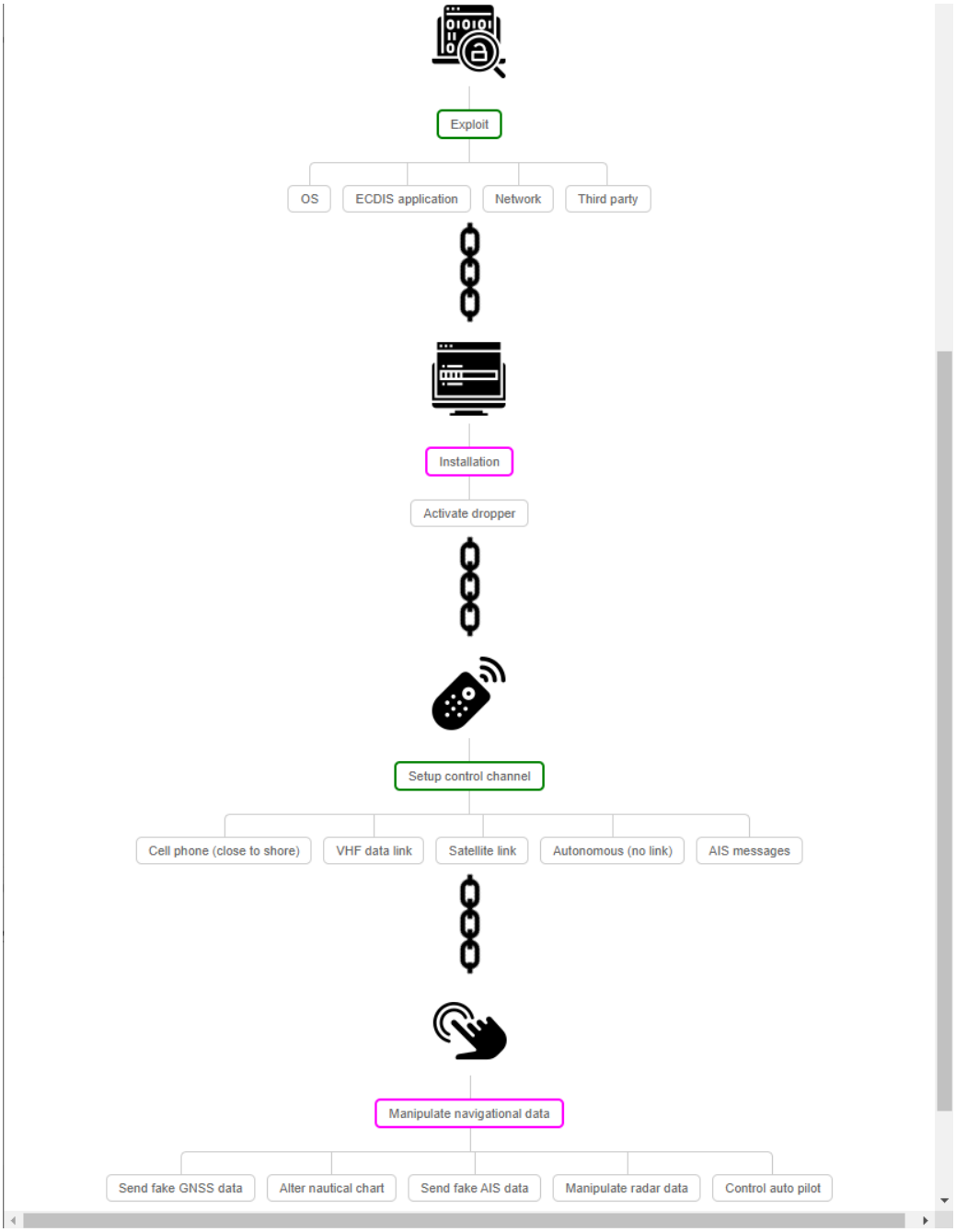


Figure 7. A screenshot from the last four stages; Exploitation, Installation, Command and Control and Actions on Objectives

The subsequent goal is to implement measures that increase these costs to a level that makes the attack unattractive, which we identify in Section 5.

4.4 Motivation

Motivation identifies the driver that causes the threat agent to commit harmful acts [26], which again helps identify the nature of the expected harmful actions. This is useful for several reasons:

- We can narrow down which targets the threat agent may focus on.
- Understanding intent help defenders focus on most likely attack scenarios.
- Security controls can be tailored to likely attack intensity and persistence.
- It is possible to direct the threat agent into traps or provide misleading information.
- Risks can be communicated in a more understandable way.

The elements in Table 13 describe all the major motivations relevant for describing a threat [26]. They are independent of each other, and any number could be assigned to one or several threat agents. These motivations should be compared against the possible consequences identified on the right side of the bow-tie diagram. Alternatively, they could be used to deduce possible consequences.

Table 13. Input to the motivation parameter

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.

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 [27]. Table 14 show examples of such intentional actions, which can be mapped to the underlying motive. The table shows extension of the objective actions presented by Casey [28].

Table 14. Intentional actions

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 [29]. 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.

4.5 Estimating threat example

As a threat estimation example, we will focus on *Compromised autonomous ship navigational system* as shown in Figure 8.

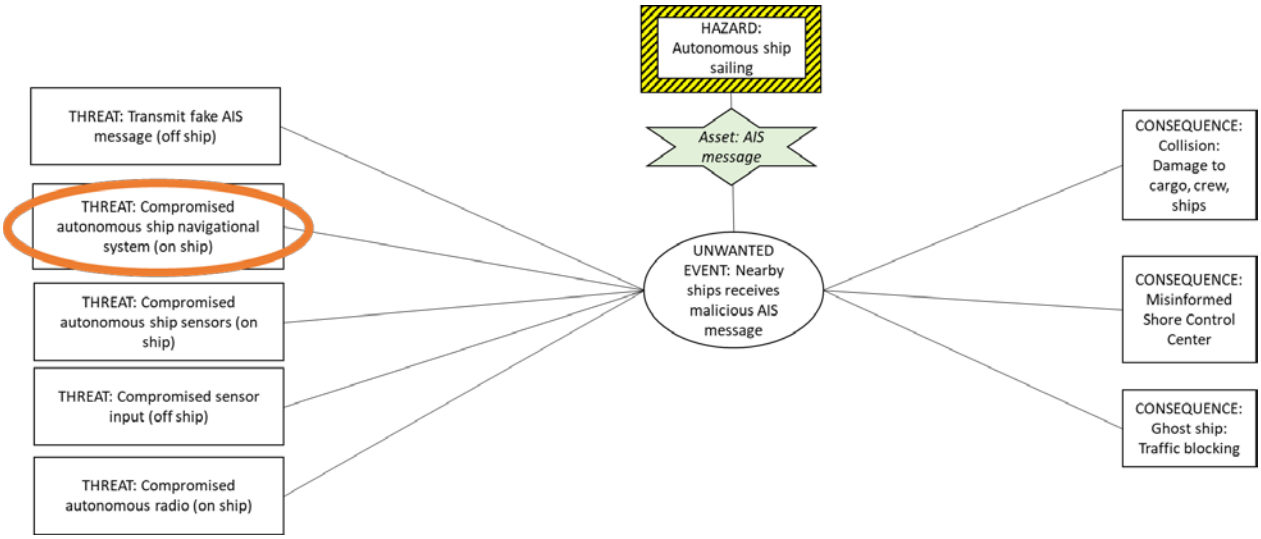


Figure 8. Threat to be estimated

This is a rather thorough example to show how an estimate can be founded on domain specific analysis data. In practice, it will probably not be necessary to dig down to this level of details for all threats, but it should be done for at least one to obtain a situational awareness before estimating the rest.

4.5.1 Threat actors

We start by identifying the threat actors that could be involved. An autonomous ship is somewhat of a special case since they are designed to operate with a minimum crew, hence we can assume a limited set of profiles as shown in Table 15. We have included "Passenger" to illustrate of a non-relevant threat agent. The *size* parameter is based on the OWASP Risk Rating Methodology [30] and indicates how large is this group of threat agents. It should be a relative number between 0 and 10. In this example there is a single Electro-technical officer onboard, several sailors, and a significant amount of pirates/criminal with online capabilities.

Table 15. Possible threat actors for the selected example threat

Affiliation	Who	Relative size weight	Justification
Onboard the autonomous ship	Electro-technical officer Sailor Passenger	1 5 0	People present on the ship during sailing and with physical access to the bridge digital infrastructure.
Within the shipping company	Technical worker	3	People with remote access to the ship from land.
System provider	Maintenance crew	3	People that visit the ship during maintenance work or have remote access.
Pirate/criminal	Cyber extortionist	8	Threat actor external to the system.
Terrorist	Unknown	2	Threat actor external to the system.
Government Cyber Warrior	Hostile neighbour state	2	Threat actor external to the system.

4.5.2 Opportunity

Since this threat will require several stages to manifest itself, there will also be varying opportunities for each of these. In Table 16 we have included four attack stages with different spatial and temporal characteristics.

Table 16. Example opportunity table

Stage	Where	When	Vulnerability
Reconnaissance	Anywhere	Anytime	NA
Weaponization	Anywhere	Anytime	NA
Delivery and installation	Anywhere	Maintenance Update software	Updates sent electronically. Use of USB interface.
Actions on objective	Congested waters	Sailing on autopilot	NA

Table 17 maps the opportunity stages with the threat agents from Table 14. What we can see here is that we cannot eliminate any of the agents based on opportunity, since there are possibilities of performing all attack stages remotely. However, we can clearly see that some agents have much better opportunities than others. The weights are relative numbers between 0 and 10 meant to indicate this.

Table 17. Mapping opportunity to threat agents

Threat agent	Opportunity	Weight	Justification
Electro-technical officer	{Reconnaissance, Weaponization, Delivery and installation, Actions on objective}	9	Always on ship and has opportunities for all stages.
Sailor	{Reconnaissance, Weaponization, Delivery and installation, Actions on objective}	9	Always on ship and has opportunities for all stages
Passenger	None	0	Not onboard the autonomous ship.
Technical worker	{Reconnaissance, Weaponization, Delivery and installation, Actions on objective}	7	Remote access to system, but not all the time. Opportunity for all stages
Maintenance crew	{Reconnaissance, Weaponization, Delivery and installation, Actions on objective}	5	Access to ship at limited time intervals (hours, days) and locations.
Cyber extortionist	{Reconnaissance, Weaponization, Delivery and installation, Actions on objective}	4	Limited window of opportunity during maintenance and software update. Done remotely unless there is an insider ally/victim.
Unknown terrorist	{Reconnaissance, Weaponization, Delivery and installation, Actions on objective}	4	Limited window of opportunity during maintenance and software update. Done remotely unless there is an insider ally/victim.
Hostile neighbour state	{Reconnaissance, Weaponization, Delivery and installation, Actions on objective}	4	Limited window of opportunity during maintenance and software update. Done remotely unless there is an insider ally/victim.

4.5.3 Means

Figure 9 shows a resource tree annotated with estimations for the costs (in $) needed to instantiate the attack. The total costs are determined by sum of all the resource costs. The resource costs are determined by the minimum and maximum costs of the resource alternatives. Table 18 summarizes the required means for each stage. The last row of Table 18 shows the minimum and maximum sum of costs for all the stages.

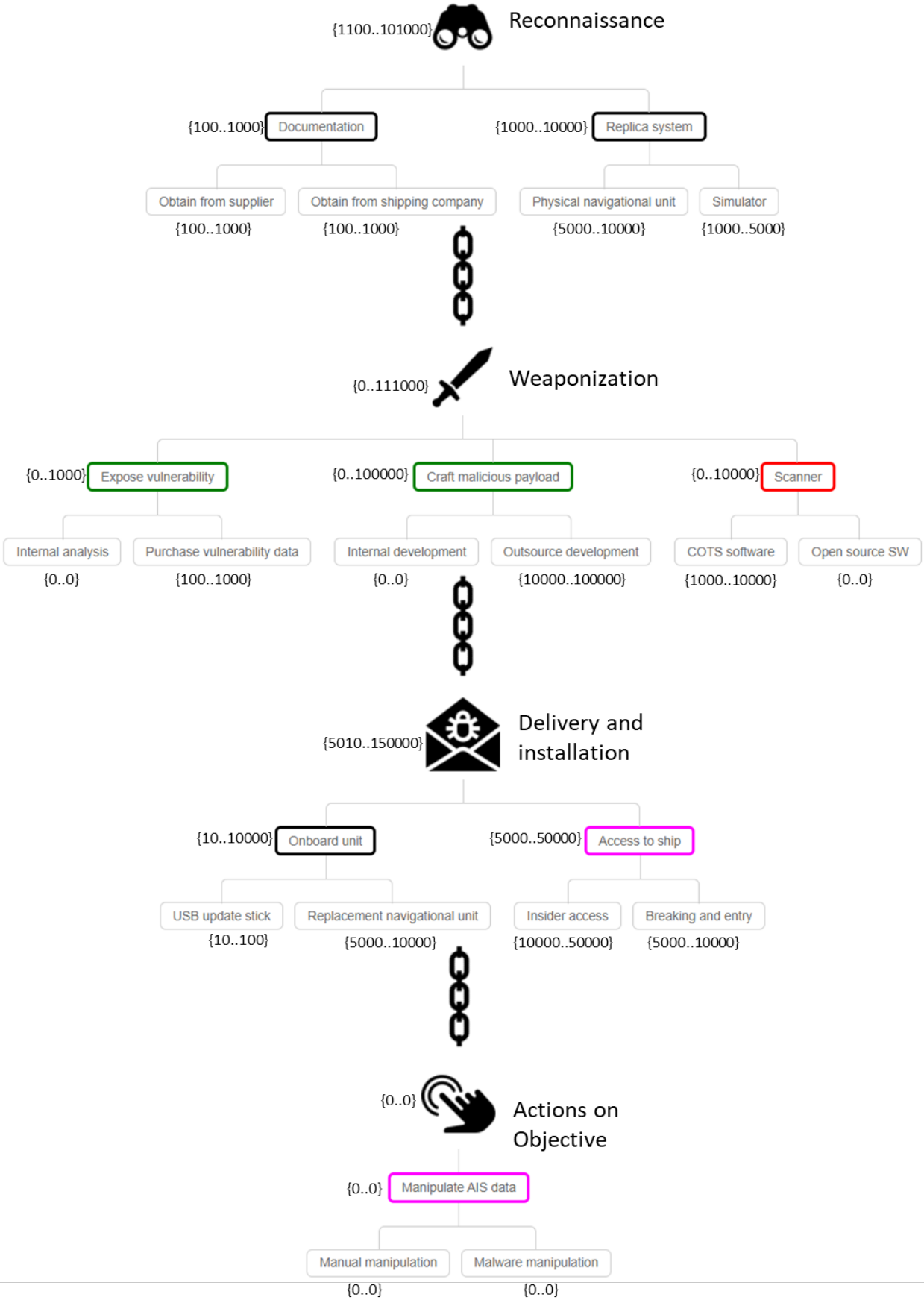


Figure 9. A four-stage resource tree with costs.

Table 18. Required means (costs)

Stage	Minimum	Maximum
Reconnaissance	1100	101000
Weaponization	0	111000
Delivery and installation	5010	150000
Actions on objective	0	0
Sum	6110	362000

In practice, there will be different resource costs for each threat actors. For instance, a sailor onboard a ship does not have to obtain means to infiltrate the ship. Therefore, we can use the means intervals from Table 17 as a lower and upper bound, and assess whether the threat actor will have the means indicated by the resource tree. In Table 19 we have used this assessment to determine a weighted value between 0 and 10 for means. A weight value of 0 indicates that the threat actor cannot obtain the required amount of resources, while a weight value of 10 indicates that the threat agent can easily obtain the required amount of resources. These weights are relative numbers. Note that in this example we have limited means to direct costs, for instance *internal development* has no costs, while outsourcing does. It would have been possible to convert a development time estimate to a monetary value, but obtaining this accurately is difficult and we are mostly interested in the minimum amount needed to assess the threat.

Table 19. Threat actors with required means

Threat agent	Means assessment	Weight
Electro-technical officer	**Reconnaissance**: In the lower segment of the estimated cost interval since the actor already has good knowledge of the target system.	9
	Weaponization: Can probably modify existing software or develop malware at a low cost.	
	Delivery and installation: No significant investment needed.	
	Actions on objective: None.	
Sailor	**Reconnaissance:** Does probably not have the means to invest in a replica system.	0
	Weaponization: Could probably not do development, does not have the available means to outsource.	
	Delivery and installation: Could possibly get access without means.	
	Actions on objective: None.	
Passenger	**Reconnaissance:** Does probably not have the means to invest in required resources.	0
	Weaponization: Could probably not do development, does not have the available means to outsource.	
	Delivery and installation: Could possibly get access without means, but might have to bribe someone on the bridge. Will need to buy a ticket.	
	Actions on objective: None.	
Technical worker	**Reconnaissance:** Already has the required resources.	9
	Weaponization: Can probably modify existing software or develop malware at a low cost.	
	Delivery and installation: No significant cost.	
	Actions on objective: None.	
Maintenance crew	**Reconnaissance:** Might need to invest in extra equipment.	8
	Weaponization: Can probably modify existing software or develop malware at a low cost.	

	Delivery and installation: No significant cost.	
	Actions on objective: None.	
Cyber extortionist	**Reconnaissance:** Non-COTS equipment is a hefty investment compared to the possible reward. Differences in ship systems makes it hard to scale up.	4
	Weaponization: Can probably modify existing software or develop malware at a low cost.	
	Delivery and installation: Might require bribing or investing in another attack-vector to deliver payload.	
	Actions on objective: None.	
Unknown terrorist	**Reconnaissance:** Must assume a well-funded terrorist.	8
	Weaponization: Must assume a well-funded terrorist.	
	Delivery and installation: Must assume a well-funded terrorist.	
	Actions on objective: None.	
Hostile neighbour state	**Reconnaissance:** State actors have close to unlimited funding and will not be hindered by investments.	9
	Weaponization: State actors have close to unlimited funding and will not be hindered by investments.	
	Delivery and installation: State actors have close to unlimited funding and will not be hindered by investments.	
	Actions on objective: None.	

4.5.4 Motivation

In Table 20 we have mapped the threat agents with motivations and intentional actions. We have given each a weight between 0 and 10 and tried to justify this estimate by considering what the actor will get out of this if the attack succeeds (reward). Similarly to the OWASP Risk Rating methodology [30], a weight close to 0 indicates that there is low or no reward, a value around 5 possible reward, and 10 a high reward.

Table 20. Possible motivation and intent for the threat actors

Threat agent	Motivation {Intent}	Weight	Justification
Electro-technical officer	Personal financial gain {Deny}	2	Little evidence that officers would try to cause damage to own ship.
Sailor	Personal financial gain {Deny}, Disgruntlement {Destroy}	2 4	Selected for the autonomous ship, trusted. Worst case: Might sabotage to preserve human jobs.
Passenger	Unpredictable {unknown}	0	No indication that passengers would want to harm the ship.
Technical worker	Personal financial gain {Deny}	2	Little evidence that shipping company employee would want to sabotage own asset.
Maintenance crew	Personal financial gain {Deny}	4	Could be 3rd party of the system provider.
Cyber extortionist	Personal financial gain {Deny}	8	Driven by financial gain.
Unknown terrorist	Unpredictable {Destroy}	5	Probably not lone wolfs. Might want to target less

			advanced ships to achieve the same goal. Worst case: Might want to cause damage to civilians and crew.
Hostile neighbour state	Dominance {Destroy}	4	At least one state that would want to demonstrate their sovereignty at sea.

4.5.5 Threat estimation summary

Having completed estimations for threat actors, their opportunity, means and motivation, we are now ready to average these values to make a combined average weight as shown in Table 21. There are many possible threat agents, and not any particular that stands out, however, *cyber extortionist* has the highest value, followed by the two insiders: *electro-technical officer* and *technical worker*. As pointed out by Williams in the OWASP Risk Rating Methodology [30], it is better to err on the side of caution and use the worst-case threat agent and that likelihood value, thus we will focus on the cyber extortionist from now on.

Table 21. Summary of threat estimation

Threat actor (role, size)		Opportunity	Means	Motivation	Average weight
Electro-technical officer	1	9	9	2	5.25
Sailor	5	9	0	4	4.5
Passenger	0	0	0	0	0
Technical worker	3	7	9	2	5.25
Maintenance crew	3	5	8	4	5
Cyber extortionist	8	4	4	8	6
Unknown terrorist	2	4	8	5	4.75
Hostile neighbour state	2	4	9	4	4.75

In Figure 10 we have updated the threat in the bow-tie diagram with visual indicators based on the worst-case threat actor from Table 20, and added similar indicators for the other threats as well (estimation process not shown). We have converted the numerical values to *traffic lights* using the mapping shown in Table 22.

Table 22. Colour conversion for the threat indicators.

Weight value	Colour code	Description
0-1		Unlikely
2-3		Possible
4-5		Likely
6-7		Almost certain
8-10		Certain

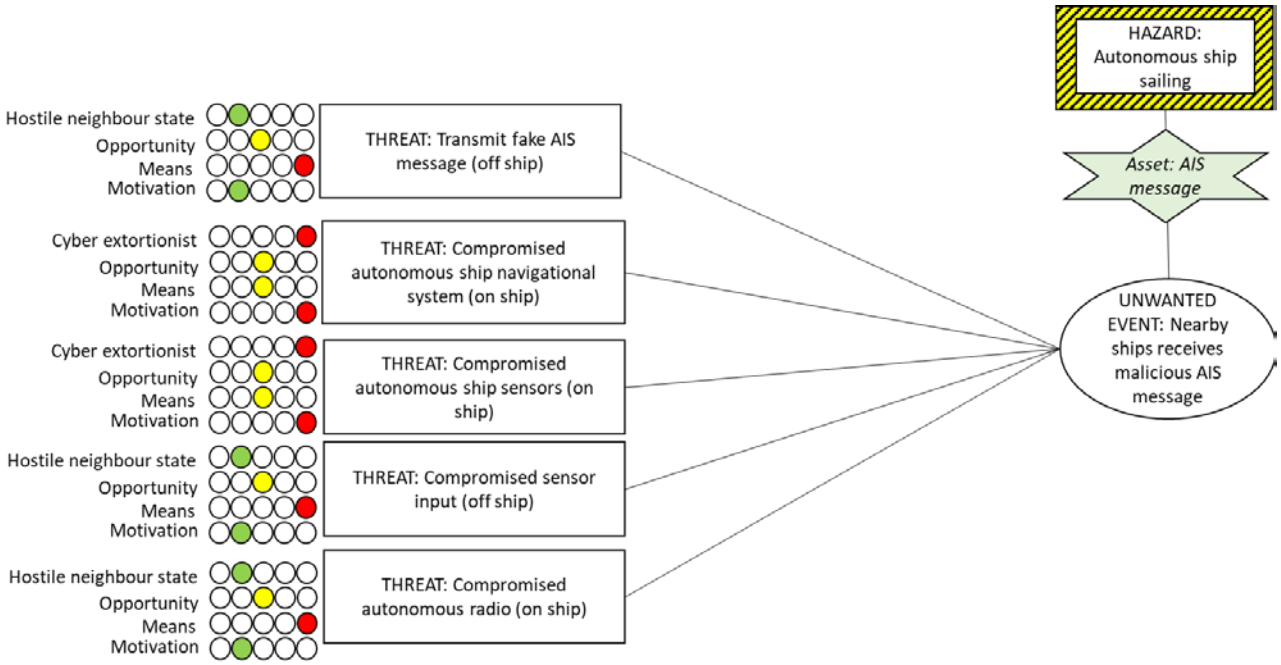


Figure 10. Left side of the bow-tie with indicators.

Having assessed and estimated each threat, we can now give an overall estimate of the likelihood or probability of the unwanted event. In order to do this, we make use of the equation developed in CySiMS and published by Bernsmed et al. [3]:

In our model, we assume that all the threats are mutually independent. This means that all the identified cyber-attacks will be executed independently of each other and that any of them can manifest itself and cause the unwanted event during the time for which the system, or service, is being assessed. Under this assumption, the probability of the unwanted event *U* can be computed as:

$$p(U) = p(at\ least\ one\ T_i\ occurs) = 1 - \prod_{i=1}^{n}\left(1 - p(T_i)\right)$$

where $p(T_i),\ i = 1 \ldots n$, is the probability of threat T_i. The problem will hence be reduced to assessing the probabilities, or likelihoods, of the individual threats that have been identified. Compared to more simplistic probability models, in which the threats are modelled as mutually exclusive (i.e. $p(U)$ will be computed as a sum of the individual threats), this is much more realistic, since it allows more threats to manifest within the same time interval, which corresponds more closely to the real world.

Table 23 shows numerical likelihood values for all the threats in the example. The probability is obtained by simply dividing the average weight by 10 to get a value between 0 and 1. There is also an overall colour indicator based on the conversion in Table 21. By applying the equation above, we get the overall likelihood as shown below.

Table 23. Likelihoods for all the threats

Identifier	Description	Indicator	Average weight	Probability
T_1	Transmit fake AIS message (off ship)		4	0.4
T_2	Compromised autonomous ship navigational system (on ship)		6	0.6
T_3	Compromised autonomous ship sensors (on ship)		6	0.6
T_4	Compromised sensor input (off ship)		4	0.4
T_5	Compromised autonomous radio (on ship)		4	0.4

$$p(U) = 1 - \big(1 - p(T_1)\big) \times \big(1 - p(T_2)\big) \times \big(1 - p(T_3)\big) \times \big(1 - p(T_4)\big) \times \big(1 - p(T_5)\big)$$
$$= 1 - (1 - 0.4) \times (1 - 0.6) \times (1 - 0.6) \times (1 - 0.4) \times (1 - 0.4) \approx 0.97$$

As can be seen from this calculation, the probability that at least one of the threats can manifest itself is close to certain within the given time frame. This is of course without any defence mechanisms in place, which we evaluate in the next section.

5 Defence mechanisms

The outcome of a security risk assessment should be *as low as reasonably practicable* ("ALARP"). In theory, there are four different approaches that can be taken to reduce risk; 1) avoid, 2) accept, 3) reduce or 4) transfer. Of these, the most commonly applied approach is to reduce risk, which means that one introduces one of more defence mechanisms, or controls, that will either reduce the likelihood or the consequence of the risk.

In the CySiMS risk assessment methodology, we include defence mechanisms in the bow-tie models as follows:

- *Preventive controls*, which reduces the likelihood of one or more identified threats. These are included as barriers in the left-hand side of the bow-tie model.
- *Detective and reactive controls*, which will reduce the consequence(s) of the unwanted event: These are included as barriers in the right-hand side of the bow-tie model.

5.1 Recommended defence mechanisms

The guidelines on cyber security onboard ships [31] provide practical recommendations on maritime cyber risk management. The document includes, amongst other things, a set of defence mechanisms, which take into account the role of personnel, procedures and technology and that have been identified as particularly relevant to equipment and data onboard ships. The identified defence mechanisms have been selected from the list of Critical Security Controls (CSC) from the Centre for Internet Security (CIS) [32]. In Table 24 we have summarized these defence mechanisms and mapped them to their application as "preventive" and/or "detective and reactive" controls in a bow-tie model. As can be seen in the table, even though most of the recommended defence mechanisms are preventive, there is also a good number of controls that are detective or reactive.

Note that the recommended defence mechanisms in [31] are mostly targeted towards existing IT systems onboard ships. Future security solutions, such as the CySiMS PKI service, are therefore not included in Table 24.

Table 24 Defence mechanisms identified in "The guidelines on cyber security onboard ships" [31]. The two columns to the right indicate whether the defence mechanisms are preventive ("P") or detective and/or reactive ("D").

Defence mechanisms (controls)		P	D
Technical protection	**Controlled networks**: • Limitation to and control of network ports, protocols and services.	X	
	Secure configurations: • Secure configuration for network devices such as firewalls, routers and switches.	X	
	Physical security: • Areas containing sensitive OT or IT control components should be securely locked. • Security and safety critical equipment and cable runs should be protected from unauthorised access. • Physical access to sensitive user equipment (such as exposed USB ports on bridge systems) should be secured.	X	

Defence mechanisms (controls)	P	D
Detection, blocking and alerts: • A baseline of network operations and expected data flows for users and systems onboard the ship should be established and managed, so that cyber incident alert thresholds can be established. • An Intrusion Detection System (IDS) may be installed in the network or as part of the ship firewall. • Onboard personnel need to understand the alerts and their potential implications.		X
Satellite and radio communication: • Uplink connections for the ship's navigation and control systems to shore-based service providers need to be protected, to prevent illegitimate connections gaining access to the onboard systems. • A firewall in front of the servers and computers connected to the networks (ashore or on board) should be deployed. • The management interface of the communication equipment must be protected.	X	
Wireless access control: • Wireless access to networks on the ship should be limited to appropriate authorised devices and secured using a strong encryption key, which is changed regularly. • Guest networks should be isolated from administrative (bridge) networks.	X	
Malware detection: • Onboard computers should be protected to the same level as office computers ashore. • Anti-virus and anti-malware software should be installed, maintained and updated on all personal work-related computers onboard.		X
Secure configuration for hardware and software: • Only senior officers should be given administrator profiles. • User profiles should be restricted to only allow the computers, workstations or servers on the ship to be used for the purposes, for which they are required. • User profiles should not allow the users on the ship to alter the systems or install and execute new programs.	X	
Email and web browser protection: Email communication between ship and shore is a vital part of a ship's operation and best practices for safe email transfer should always be followed. This includes • Email as zip or encrypted file when necessary. • Disable hyperlinks on email system used onboard. • Avoid using generic email addresses for the personnel onboard.	X	
Data recovery capabilities: • Ensure that essential information and software on the ships are being backed-up. • Restore scenarios should be established to prioritise which critical onboard systems need quick restore capabilities to reduce the impact. • Onboard systems that have high data availability requirements should be made resilient. • OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber incident.		X

Defence mechanisms (controls)		P	D
	Application software security (patch management): • Safety and security updates should be provided to onboard systems. • Ordinary security patches should be included in the ship's periodic maintenance cycle. • Critical patches should be evaluated in terms of operational impact on the OT systems. These updates or patches should be applied correctly and in a timely manner. • If a critical patch cannot be installed, alternative measures should be evaluated to help implement virtual patching techniques.	X	
Procedural protection measures	**Training and awareness**: • Training and awareness should be tailored to the appropriate levels for onboard personnel including the master, officers and crew[1]. The awareness programme should cover scenarios relevant onboard, including • Risks related to the use of own devices onboard. • Risks related to installing software of the ship computers. • Risks related to the physical presence of non-company personnel, for example where third-party technicians are left to work on equipment without supervision • Detecting and reporting suspicious activity, for example someone plugging in an unknown device on the ship network. • Awareness of the consequences or impact of cyber incidents to the safety and operations of the ship. • Understanding how to implement preventative maintenance routines such as anti-virus, patching and backups on the ship. • Procedures for protection against risks from service providers' removable media before connecting to the ship's systems.	X	X
	Access for visitors: • Visitors such as authorities, technicians, agents, port and terminal officials, and owner representatives should be restricted with regard to computer access whilst on board. • Unauthorised access to sensitive OT network computers by visitors should be prohibited. • If access to a network by a visitor is required and allowed, then it should be restricted in terms of user privileges. • Access to certain networks for maintenance reasons should be approved and co-ordinated following appropriate procedures as outlined by the company/ship operator. • If a visitor requires computer and printer access, an independent computer, which is air-gapped from all controlled networks, should be used.	X	

[1] Training and awareness should also cover collaboration between IT and crew in order to enhance their understanding of their roles and responsibilities, as well as the possible consequences their actions might lead to.

Defence mechanisms (controls)	P	D
Upgrades and software maintenance: • Relevant hardware and software installations on board should be updated to help maintain a sufficient level of security. • Procedures for timely updating of software may need to be put in place taking into account the ship type, speed of internet connectivity, sea time, etc. • Routers, switches and firewalls, and various OT devices will be running their own firmware and may also require regular updates. • Scanning software tools that detect and deal with malware also need to be updated.	X	X
Remote access: • Policy and procedures should be established for control over remote access to onboard IT and OT systems. • Clear guidelines should establish who has permission to access, when they can access, and what they can access. • Any procedures for remote access should include close co-ordination with the ship's master and other key senior ship personnel. • All remote access occurrences should be recorded for review in case of a disruption to an IT or OT system. • Systems, which require remote access, should be clearly defined, monitored and reviewed periodically.	X	
Use of administrator privileges: • Access to information should only be allowed to relevant authorised personnel • Administrator privileges should only be given to appropriately trained personnel, who as part of their role in the company or on board, need to log onto systems using these privileges. • User privileges should be removed when the people concerned are no longer on board.	X	
Physical and removable media controls: • There should be a procedure in place to check removable media for malware and/or validate legitimate software by digital signatures and watermarks. • Policies and procedures for removable media usage should include a requirement to scan any removable media device in a computer that is not connected to the ship's controlled network. • Wherever possible, the files and forms should be transferred electronically or be downloaded directly from a trusted source without using removable media.	X	
Equipment disposal, including data destruction: • The company should have a procedure in place to ensure that the data held in obsolete equipment is properly destroyed and cannot be retrieved.	X	
Obtaining support from ashore and contingency plans: • Ships should have access to technical support in the event of a cyber-attack. • Details of this support and associated procedures should be available on board.		X

5.2 Cost-efficient protection

To ensure a cost-efficient protection against cyber-attacks, it is desired to do a cost-benefit analysis (CBA) of the identified defence mechanisms (controls) before they are implemented. A rule of thumb in information security is to not spend more to protect an asset than the value of that asset. However, this does not apply when doing cyber security risk assessment of safety critical systems, because the consequences of unwanted events may have safety implications beyond the identified asset, such as physical damages to ships, to shore-

side constructions, to the environment and even loss of human life. We therefore need to focus on the expected loss associated with the identified consequences in the bow-tie diagram when we do the cost-benefit analysis.

Table 25 outlines the cost factors that we use to compute the cost-benefit of a control.

Table 25 Cost-benefit analysis of controls: cost factors. Adapted from [33].

Cost factor	Note
Single Loss Expectancy (SLE)	The average cost associated with a single occurrence of the consequence. • For preventive controls: select the cost associated with the *worst-case* consequence in the bow-tie model. • For detective and reactive controls: select the cost associated with the consequence in the bow-tie model that the control intends to mitigate.
Annual Rate of Occurrence (ARO)	An estimation of how often the unwanted event is expected to happen each year. • For preventive controls: estimate the likelihood of the *threat* that is causing the unwanted event (see Section 4). • For detective and reactive controls: estimate the likelihood that the unwanted event will manifest into the consequence (see Section 4).
Annual Loss Expectance (ALE)	The expected yearly cost associated with the consequence. Can be computed as ALE=SLE*ARO.
Annual cost of control (COST)	The expected yearly cost to deploy and operate the control.
Annual Loss Expectancy, before control (ALEpre)	The expected yearly cost associated with the consequence *before* the control has been implemented. Will be computed in the same manner as ALE.
Annual Loss Expectancy, after control (ALEpost)	The expected yearly cost associated with the consequence *after* the control has been implemented. Will be computed in the same manner as ALE.

The cost-benefit can then be computed by subtracting the cost of the control (COST) from the difference between the expected yearly cost associated with the consequence before the control has been implemented (ALEpre) and the expected yearly cost associated with the consequence after the control has been implemented (ALEpost). Equation 1 shows how to compute the cost-benefit of a control.

Equation 1: Computing the cost-benefit of a control

$$Cost - benefit = (\text{ALEpre} - \text{ALEpost}) - \text{COST}$$

The cost-benefit is hence the amount of money that the control is saving the company, taking the cost of the control itself into account.

Note that the intention of doing the cost-benefit analysis may not only be to provide good estimates of costs and benefits, but it can also help in prioritizing between different controls

5.3 Cost-benefit analysis in the autonomous ship use case

An example of a cost-benefit analysis of a *preventive* control is provided in Figure 11. Here we want to do a cost-benefit analysis (CBA) of a potential control for preventing the threat "Compromised autonomous ship navigation system (on ship)", which may cause the unwanted event "Nearby ships receives malicious AIS messages" in the autonomous ship use case. The identified control C1 is "Digital signatures of software updates", which is one of the services that the CySiMS PKI service intends to provide. In our assessment, we are doing the CBA with the intention to prevent the consequence "Collision: Damage to cargo, crew and ship", which is the worst-case outcome in this scenario. The cost values shown here are illustrative and can include direct costs and cost for development/operating/maintenance.

In the CBA, we use the following numbers to assess the costs:

- Single Loss Expectancy (SLE) = $100 000
- Annual cost of control (COST) = $500, which approximates the yearly cost per ship for a digital signature solution (such as the CySiM PKI) for securing software updates to the navigational system.

We then assume that the introduction of the control will reduce the likelihood of the threat from once every second year to once every fifth year.

- Annual Rate of Occurrence (ARO) = 0.5 (before control) and 0.2 (after control).

We can now compute

- Annual Loss Expectancy, before control (ALEpre) = $100 000 * 0.5 = $50 000
- Annual Loss Expectancy, after control (ALEpost) = $100 000 * 0.2 = $20 000
- Cost-benefit = (ALEpre – ALEpost) – COST = $50 000 - $20 000 - $500 = $29 500

The cost-benefit analysis hence indicates that the amount of money that a digital signature scheme such as the PKI service will be saving the company, taking the cost of deploying and operating the service onto the ship into account, will be approximately $29 500.

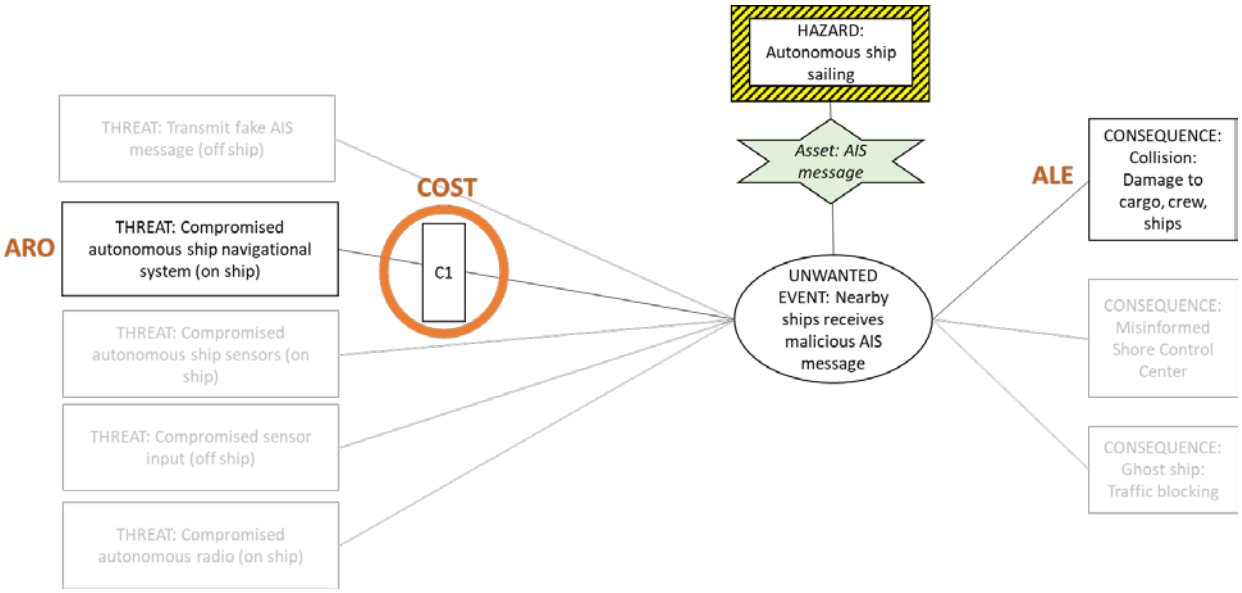


Figure 11 Cost-benefit analysis of a preventive control (C1).

An example of a cost-benefit analysis of a *reactive* control is provided in Figure 12. Here we want to do a CBA of a potential control for reacting to the unwanted event "Nearby ships receives malicious AIS messages"

in the autonomous ship use case. The identified control C2 is "Training and awareness" from Table 23, with specific focus on "awareness of the consequences or impact of cyber incidents to the safety and operations of the ship." Similar as for the preventive control, the intention of this reactive control is to prevent the consequence "Collision: Damage to cargo, crew and ship".

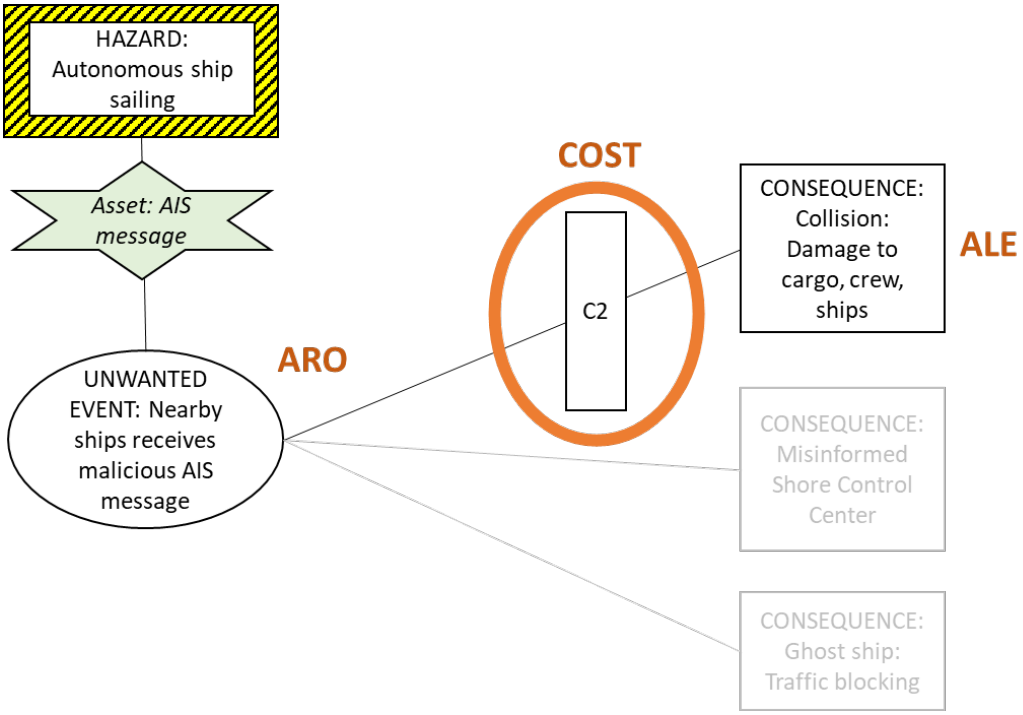


Figure 12: Cost-benefit analysis of a reactive control (C2).

In the CBA, we use the following numbers to assess the costs:

- Single Loss Expectancy (SLE) = $100 000
- Annual cost of control (COST) = $10 000, which is an approximation of the yearly cost of running a relevant awareness program for the relevant employees in the organization.

We then assume that the introduction of the control will reduce the likelihood that the unwanted event causes the consequence "Collision" from once every second year to once every third year.

- Annual Rate of Occurrence (ARO) = 0.5 (before control) and 0.33 (after control)

We can now compute

- Annual Loss Expectancy, before control (ALEpre) = $100 000 * 0.5 = $50 000
- Annual Loss Expectancy, after control (ALEpost) = $100 000 * 0.33 = $33 000
- Cost-benefit = (ALEpre – ALEpost) – COST = $50 000 - $33 000 - $10000 = -$7 000

The cost-benefit analysis hence indicates that the amount of money that the control "Training and awareness" is saving the company, taking the cost of running the awareness program into account will be approximately $7 000.

5.4 Preventive versus reactive controls

Sometime there is a trade-off to be made, in the selection between different types of controls. This trade-off is not only related to the selection between two (or more) different controls that serve the same purpose, but also whether one should go for detective and reactive controls, instead of, or in addition to, preventive controls. Preventive controls, which are modelled in the left-hand side of the bow-tie, are intended to reduce the likelihood of the unwanted event, by mitigating the threats that one has foreseen can cause the unwanted event. On the other hand, detective and reactive controls which are modelled in the right-hand side of the bow-tie, will reduce the consequences of the unwanted events. While the selection between two or more preventive controls can be viewed as a design-choice, the selection between preventive controls and reactive controls can be seen as a more strategic choice, *moving the focus to preparedness, rather than prevention.*

Cyber security has traditionally been mostly focused on preventive controls; however, it is nowadays widely accepted that it is both difficult and expensive to prevents all kind of incidents from happening. In some cases, it may therefore be better to allow the unwanted event to happen and instead be prepared to deal with it once it happens. This calls for an increased focus of the detective and reactive controls in the bow-tie models.

The cost-benefit analysis (CBA) method that we have outline in this report can be used to aid the decision making in such trade-offs. For example, in the autonomous use case (section 5.3) we showed that the preventive control "PKI service" will save the company approximately $29 500 whereas the reactive control "Training and awareness" will only save the company $7 000. Here the CBA indicates that it might be better to go for the preventive control.

5.5 Resilience

Defence mechanisms (controls) are in most cases selected and implemented with the intention of countering known threats, and known unwanted events, which are caused by threats that have been foreseen, modelled and assessed during a risk assessment, such as our bow-tie modelling approach. However, during the last few years, *resilience* has emerged as a new topic in the maritime industry. In the "Code of Practice: Cyber Security for Ships" [34], resilience is defined as "*the ability to adapt, respond and recover rapidly from disruptions and maintain continuity of business operations*". The same document also points out that "*in the event of a security incident, it is vital that the ship is able to respond and recover rapidly, so that it can continue operating without disruption or compromise to the services that it provide to its users*". Being resilient implies that one also expects the unexpected and knows how to respond.[2] This clearly emphasizes the need to focus more on detective and reactive controls, to minimize the impacts of all kinds of unwanted events.

To be resilient, the "Code of Practice: Cyber Security for Ships" [34] suggests that a ship needs to have in place an incident management plan which is based upon an understanding of :

- the potential causes of disruption, cyber, human and natural;
- the essential systems required to keep the ship operating safely;
- the nature and practicality of alternative methods which can be employed in the
- event of an incident to maintain operations; and
- the capacity at which the ship can realistically operate under such arrangement

The guidelines on cyber security onboard ships [31] takes a similar standpoint as [34], pointing out that "*appropriate contingency plans for cyber incidents, including the loss of critical systems and the need to use alternative modes of operation, should be addressed by the relevant operational and emergency procedures included in the safety management system.*" Relevant defence mechanisms (controls) for the right-hand side of the bow-tie model may therefore already exist in the ships' safety management system.

[2] The phrase "*expecting the unexpected and know how to respond*" was coined by the H2020-EU.3.7 research project DARWIN (2015-2018). https://cordis.europa.eu/project/id/653289

The bow-tie modelling approach is, in itself, providing some degree of resilience, because it puts focus on the right-hand side consequences and mitigating controls. But one also needs to invest in the unforeseen. Most importantly, critical systems and critical operations on the ship will need to continue operate uninterrupted, despite unwanted events that we did not foresee.

6 References

1. Nesheim, D.A., et al., *D1.1 Risk Model and Analysis*. 2017, SINTEF: http://cysims.no/.
2. *D1.2 Risk assessment tool*. 2018, SINTEF: CySiMS.
3. Bernsmed, K., et al. *Visualizing cyber security risks with bow-tie diagrams*. in *International Workshop on Graphical Models for Security*. 2017. Springer.
4. Meland, P.H., et al., *An experimental evaluation of bow-tie analysis for cybersecurity requirements*, in *Computer Security*. 2018, Springer. p. 173-191.
5. Meland, P.H., et al., *An experimental evaluation of bow-tie analysis for security*. Information & Computer Security, 2019.
6. *BowTiePlus*. 2017, GitHub.
7. Rossi, P., et al., *CYBER SECURITY BY DESIGN*. 2018, DNV-GL.
8. Shinder, D.L. and M. Cross, *Scene of the Cybercrime*. 2008: Elsevier.
9. Nykodym, N., R. Taylor, and J. Vilela, *Criminal profiling and insider cyber crime.* Computer Law & Security Review, 2005. **21**(5): p. 408-414.
10. Warikoo, A., *Proposed methodology for cyber criminal profiling.* Information Security Journal: A Global Perspective, 2014. **23**(4-6): p. 172-178.
11. AAPA. *Glossary of Maritime Terms*. 2020 [cited 2020 18 May]; Available from: https://www.aapa-ports.org/advocating/content.aspx?ItemNumber=21500.
12. Wikipedia. *Seafarer's professions and ranks*. 2020 [cited 2020 18 May]; Available from: https://en.wikipedia.org/wiki/Seafarer%27s_professions_and_ranks.
13. Wikipedia. *International Ship and Port Facility Security Code*. 2020 [cited 2020 18 May]; Available from: https://en.wikipedia.org/wiki/International_Ship_and_Port_Facility_Security_Code.
14. Dubay, D. *Why We Will Never See Fully Autonomous Commercial Ships*. 2019 June 25 [cited 2020 May 29]; Available from: https://www.maritime-executive.com/editorials/why-we-will-never-see-fully-autonomous-commercial-ships.
15. Wikipedia. *Marine surveyor*. 2020 [cited 2020 18 May]; Available from: https://en.wikipedia.org/wiki/Marine_surveyor.
16. EU. *What is a data controller or a data processor?* 2020 [cited 2020 18 May]; Available from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en.
17. Winner, A.C., P. Schneider, and A.T. Weldemichael, *Maritime terrorism and piracy in the Indian Ocean Region*. 2012, Taylor & Francis.
18. Pendse, S.G., *Ethical hazards: A motive, means, and opportunity approach to curbing corporate unethical behavior.* Journal of Business Ethics, 2012. **107**(3): p. 265-279.
19. Van Ruitenbeek, E., et al. *Characterizing the behavior of cyber adversaries: The means, motive, and opportunity of cyberattacks*. in *40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Supplemental (DSN 2010)*. 2010.
20. McKendall, M.A. and J.A. Wagner III, *Motive, opportunity, choice, and corporate illegality.* Organization Science, 1997. **8**(6): p. 624-647.
21. Haga, K., P.H. Meland, and G. Sindre. *Breaking the cyber kill chain by modelling resource costs*. in *The Seventh International Workshop on Graphical Models for Security (GraMSec 2020)*. 2020. Springer.
22. Hutchins, E.M., *The cyber kill chain*. 2020, Lockheed Martin.
23. Schneier, B., *Attack trees.* Dr. Dobb's journal, 1999. **24**(12): p. 21-29.
24. Pols, P., *The Unified Kill Chain: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks.* Cyber Security Academy, 2017.
25. Lund, M.S., O.S. Hareide, and Ø. Jøsok, *An attack on an integrated navigation system.* Necesse 2018. **3**(2).
26. Casey, T., *Understanding cyber threat motivations to improve defense.* Intel White Paper, 2015.

27. *Is There a Difference Between Intent and Motive?* 2019 June 19 [cited 2020 27 May]; Available from: https://www.thewebsterlawoffice.com/blog/2019/june/is-there-a-difference-between-intent-and-motive-/.
28. Casey, T., *Threat Agent Library Helps Identify Information Security Risks*. 2007, Intel.
29. FARRAR, C., H. SOHN, and G. PARK. *Converting large sensor array data into structural health information*. in *The 4th International Workshop on Structural Control*. 2005. DEStech Publications, Inc.
30. Williams, J. *OWASP Risk Rating Methodology*. 2020 [cited 2020 19 May]; Available from: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.
31. BIMCO, *THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, version 3*. 2018, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, WORLD SHIPPING COUNCIL.
32. CIS, *Critical Security Controls for Effective Cyber Security, v7.1*. 2019.
33. Wilson, D. *Justifying Security: Cost Benefit Analysis*. 2017 [cited 2020 June 5]; Available from: http://concernednerds.com/justifying-security-cost-benefit-analysis/
34. IET, *Code of Practice: Cyber Security for Ships.* . 2017, Department for Transport, UK.

A Appendix A

Threat Actor: Negligent Insider	
Access: Internal Limits: Legal Resources: Individual	Skills: Operational Visibility: Covert Intent: Non-hostile
Summary: Negligence or lack of proper training might make otherwise loyal and trustworthy employees a threat to the ecosystem/company. Their main intention is to solve everyday tasks without any perceived obstacles put in place by the organisations security policy. **Activity**: Negligent insiders is a recurring problem with little improvements over the last years. These trusted and loyal employees circumvent the established rules and procedures, because of e.g. lack of knowledge, efficiency, laziness or simplicity, in order to get their work done. The capacity of the negligent insider is high, but not being determined to cause harm introduces some randomness to which data or access is lost. **Target**: The negligent insider does not actively target an organisation, but by way of negligence, he can cause the same amount harm. **Evaluation Considerations**: To be completed for each use of the framework	

Threat Actor: Government Cyber Warrior	
Access: External Limits: Extra-legal, major Resources: Government	Skills: Adept Visibility: Multiple / Don't care Intent: Hostile
Summary: The never halting race for military power and advantage makes governments a highly motivated threat actor. Disrupting the shipping operations of a country or region might serve to demonstrate such capacity and power. In the event of a military conflict, gaining control of the opponent's national fleet might be of strategic importance. **Activity**: Depending on the country, the capacity is very high. Some countries even have large military divisions dedicated to cyber-warfare. Even for a small country like Norway the Cyber Defence Force accounts for 7 % of its active military personnel. NSA, in the US, and 3PLA, in China, has considerable capabilities with regard to both personnel, technical expertise and finance. The 3PLA is estimated to employ more than 100 000 persons. **Target**: In many regions, any disruption to the shipping traffic would soon have large ramifications on the economy of the area. Industries relying on materials would come to halt; logistics of transporting goods within a country would be more cumbersome – potentially affecting their ability to fend off a conventional attack. **Evaluation Considerations**: To be completed for each use of the framework	

Threat Actor: Government Spy	
Access: External Limits: Extra-legal, major Resources: Government	Skills: Adept Visibility: Clandestine Intent: Hostile
Summary: Developing technology is expensive. Some countries use government intelligence services to obtain new technology for their national industry. Governments are also interested in learning more about the people and technologies of businesses for general surveillance purposes. **Activity**: Depending on the country, the capacity is very high. Some countries even have large military divisions dedicated to cyber-warfare. Even for a small country like Norway the Cyber Defence Force accounts for 7 % of its active military personnel. NSA, in the US, and 3PLA, in China, has considerable capabilities with regard to both personnel, technical expertise and finance. The 3PLA is estimated to employ more than 100 000 persons. **Target**: The shipping industry is increasingly high tech and performing advanced operations. The motivation for targeting the industry can range from wanting to know more about the technology in use, to wanting access to data collected by the vessel or about cargo and passengers. By obtaining this information by means of digital espionage, the perpetrator runs less of a risk of detection as well as reduces the cost of the operation. **Evaluation Considerations**: To be completed for each use of the framework	

Threat Actor: Script kiddie	
Access: External Limits: Extra-legal, minor Resources: Individual	Skills: Minimal Visibility: Overt Intent: Hostile
Summary: Script kiddies utilizes pre-created software and scripts to direct attacks at a target. The script kiddies could be young, aspiring hackers trying to learn the game and make a name for themselves. **Activity**: The number of tools available for hacking, makes it possible for such an actor to be somewhat effective against system with lacking security. However, they usually lack the expertise to modify scripts to a different context than the one they were originally created for. This lack of expertise also prevents the script kiddie from fully exploiting the information he obtains and the systems in question. **Target**: A script kiddie will generally not have any reason for targeting a particular actor, but the attack is often one of convenience. **Evaluation Considerations**: To be completed for each use of the framework	

Threat Actor: Security researcher	
Access: External Limits: Code of Conduct Resources: Individual	Skills: Adept Visibility: Overt Intent: Non-hostile

Summary: Highly skilled individuals might attack the system in order to find new flaws and thus intentionally or unintentionally cause service disruption. They could be motivated by the mental challenge, prospect of fame or the possibility to prove their skills.

Activity: The security research community has grown significantly over the past years, with e.g. young researchers eager to prove their worth and win their fame by means of discovering vulnerabilities. It is also increasingly common for companies to use the discovery of vulnerabilities as opportunities to market their own services through professional branding and exaggeration of the vulnerability in the media.

Target: The security researcher will often target high profile targets in order to obtain the highest possible public exposure of his findings. Other researchers might be motivated by the greater good and primarily target systems and installations they perceive as critical infrastructure

Evaluation Considerations: To be completed for each use of the framework

Threat Actor: Pirate / Criminal	
Access: External Limits: Extra-legal, major Resources: Organisation	Skills: Operational Visibility: Covert Intent: Hostile

Summary: Criminals will always find new ways in which they can enrich themselves. If this can be done through posing a threat to an industry, there is a real possibility that someone will explore the option.

Activity: Traditionally, piracy and criminal activity against the shipping industry has been physical assaults either at sea or in port. At the coast of Nigeria, there have been multiple piracy attacks. In the later years, we have also seen modern piracy take form by means of e.g. ransomware. This reduces the exposure of the involved parties, gives high return of investment and gives a broader reach. The capability is believed to be high amongst organised criminals, with e.g. Mexican drug cartels allegedly recruiting/kidnapping hackers and cyber specialists.

Target: A criminal could benefit from posing a threat to an industry in multiple ways. If able to either disrupt the operations, the perpetrator could demand a ransom for restoring normal operations. The perpetrator could steal information or force/trick a ship to a place where he could steal either cargo, the entire ship, or have a ship transport goods on his behalf. A more sophisticated exploitation by a criminal could be to manipulate the stock market[3]. Over time, the maritime industry has established a precedence for paying ransom in the event of piracy with 85 % of all hijacked vessels paying ransom. There are currently no reasons to believe that the situation will be significantly different with digital piracy, since the will to pay has already been established.

Evaluation Considerations: To be completed for each use of the framework

[3] Sell short in a company, make the stock price plummet and make a profit. (Extreme version of short and distort) Buy long in a company, deface competitors and make a profit. (Extreme version of pump and dump)

Threat Actor: Activist hacker	
Access: External Limits: Extra-legal, major Resources: Team	Skills: Operational Visibility: Overt Intent: Hostile
Summary: Two or more hackers/script kiddies collaborating on one or several attacks in order to promote a cause. The motivation for targeting the maritime industry depends on the cause which they promote. **Activity**: Some activist hacker groups have demonstrated some capacity, like Anonymous, for DDoS and other simple attacks. Though the media hype could lead to believe hacktivist groups to have extremely high capability, the groups' capabilities are believed to be fairly low in addition to the groups being less unified than a common name and term suggests. **Target**: Regular activists have targeted the maritime industry for a long time, for causes such as the environment, animal protection or any number of other causes. If able to fight for their cause by means of cyber-attacks, the activists are likely to utilise hacktivism as well as regular activism. The hacktivism can be directed at specific vessels or companies, but also ports and nations. **Evaluation Considerations**: To be completed for each use of the framework	

Threat Actor: Former employee	
Access: External Limits: Extra-legal, minor Resources: Individual	Skills: Operational Visibility: Covert Intent: Hostile
Summary: This is mostly the same as for the malicious insiders if no routine exists for removing access upon leaving the company. If routines for removing access are in place and executed correctly, the perpetrators capability is reduced. The perpetrator will still have extensive knowledge about the systems and their configuration, but will have to obtain access through other means than using his own. **Activity**: Former employees comes in at least two flavours: disgruntled and just former. The disgruntled employees have long been active in the media and badmouthing the former employer. Their resources to harm their former employer might not be the largest, but their resentment might be a strong motivating factor. The former employees have taken relevant and confidential information when leaving for another company – some even aver quitting. **Target**: There are examples of former employees, who still have access to their former employers' systems, who take whatever information they need to become more successful working for a competitor. Furthermore, even without direct access to the systems of the former employer, a disgruntled former employee have a large amount of information about the systems and people at the company so that he can cause a great deal of harm by knowing which systems to attack and which buttons to press on his former co-workers. **Evaluation Considerations**: To be completed for each use of the framework	

Threat Actor: Terrorist	
Access: External Limits: Extra-legal, major Resources: Organisation	Skills: Operational Visibility: Covert Intent: Hostile

Summary: Over the last couple of years, terrorist organisations have demonstrated their commitment and high motivation for their cause – although said causes differ.

Activity: Terrorist organisations have been very active over the past years, primarily by means of physical attacks and scare mongering, but they are moving in the direction of cyber attacks as well. As of the beginning of 2016, the currently most famous terrorist organisation known as ISIS is not believed to have the necessary capabilities to perform serious cyber attacks themselves, but analysts believe they are working on cultivating or obtaining the relevant skills. While waiting to obtain such skills, ISIS is using external competence like when the group allegedly used Ardit Ferizi to obtain personal information on US military and government personnel. ISIS has the financial means to hire the required personnel and competence on e.g. the dark web. In Pakistan, Lashkar-e-Taiba focuses mainly on using its technical and cyber expertise to guard their communication. Still, the group recruits directly from some of the best Pakistani universities and offers better salary than local companies.

Target:
There have been multiple examples throughout time that the maritime domain is of interest for terrorists. The economic, societal and fear inducing effect is clear. Traditionally, ships have been moving relatively slowly and, despite ISPS being an improvement, quite accessible to terrorists. This appears to hold true also for the cyber domain. Furthermore, terrorists are not merely of a specific race or from a specific area, there is a possibility of insiders either being a terrorist or assisting terrorists – either of free will or extortion.

Evaluation Considerations: To be completed for each use of the framework

Threat Actor: Competing Shipping Company	
Access: External Limits: Extra-legal, minor Resources: Organisation	Skills: Adept Visibility: Clandestine Intent: Hostile

Summary: Shipping is a competitive industry and some actors might turn to hostile methods in order to increase their profits. Knowing the industry and the systems, they make a noteworthy adversary.

Activity: In most every industry with fierce competition, espionage, sabotage, and poaching of employees are known phenomena. In some parts of the world, there are strong ties between national industry and the government, giving the companies stronger capabilities with regard to espionage.

Target: Shipping companies maintain large collections of business sensitive data regarding goods, customers and operations. Access to such data could prove very profitable for a competitor if used to either deface the company or steal their customers by knowing exactly which offers to put to a customer. The competitor could also attract insiders to do their bidding by offering them economic compensation or the prospect of a job after the deed is done.

Evaluation Considerations: To be completed for each use of the framework