NTNU

Norwegian University of
Science and Technology

Perceived Information Security in the Maritime Sector

Roy Skoglund

Master in Information Security	
Submission date:	December 2017
Supervisor:	Slobodan Petrovic, IIK
Co-supervisor:	Christian Frøystad, SINTEF Karin Bernsmed, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Preface

This report constitutes the written examination in the course MIS4900: Master's Thesis – Information Security. The thesis will conclude the author's Master of Science in Information Security, specializing in Management. It has been written part time in the spring and autumn semesters of 2017, at the Norwegian University of Science and Technology's (NTNU) Faculty of Information Technology and Electrical Engineering. The thesis has been written in cooperation with SINTEF, which has been very helpful in the process of formulating an initial problem that a thesis could be built on.

15-12-2017

Acknowledgment

This thesis has been written in cooperation with SINTEF. Slobodan Petrovic has been the local supervisor at NTNU, while Christian Frøystad and Karin Bernsmed has been the external supervisors at SINTEF. I would like to use this opportunity to thank them all for their guidance and contributions.

R.S.

Abstract

The maritime sector is increasingly dependent on digital systems; systems that in many cases was initially designed without security in mind. At the same time, it is reported that the levels of information security awareness within the sector is low to non-existing. It is reported that low levels of information security awareness, and security issues with GNSS and AIS, are among the top 10 digital vulnerabilities within the maritime sector. There are several examples of how scientists have proven that the wireless systems can be manipulated, and how. This thesis, named Perceived Information Security in the Maritime Sector, aims to uncover the relationship between actual security in GPS and AIS, and how the stakeholders within the sector consider it to be. The initial hypothesis was that the considered security is higher than the actual security. To be able to view the trends of the sector, a survey was used to measure the respondent's views on GPS and AIS. The data gathered from the survey indicates that the stakeholders of the maritime sector is somewhat over-confident about both system security and potential impact if the systems are compromised.

Contents

Preface . . . . **i**
Acknowledgment . . . . **iii**
Abstract . . . . **v**
Contents . . . . **vii**
List of Figures . . . . **ix**
1 Introduction **1**
1.1 Problem Description 1
1.2 Research Questions 1
2 Basic concepts and previous work **3**
2.1 GPS (Global Positioning System) 3
2.1.1 Jamming 3
2.1.2 Spoofing 5
2.2 AIS (Automatic Identification System) 6
2.2.1 Ship Spoofing 7
2.2.2 AtoN Spoofing 7
2.2.3 Collision Spoofing (CPA) 7
2.2.4 AIS-SART Spoofing 7
2.2.5 Weather Forecasting 7
2.2.6 AIS Hijacking 8
2.2.7 Availability Disruption Threats 8
2.2.8 The Experiments 8
2.3 Similar projects 10
3 The survey **11**
3.1 Survey 11
3.1.1 Data requirements 11
3.1.2 Data generation method 11
3.1.3 Sampling frame 12
3.1.4 Sampling technique 12
3.1.5 Response rate and non-responses 12
3.1.6 Sample size 12
3.2 Questionnaire 13
3.3 Research ethics 16
3.3.1 Right not to participate 17

3.3.2 Right to withdraw 17
3.3.3 Right to give informed consent 17
3.3.4 Right to anonymity and confidentiality 17
3.4 Analysis 18
4 Results 21
4.1 Distribution 21
4.2 Data 21
4.2.1 Factual data 21
4.2.2 Opinions 25
5 Analysis and Discussion 37
5.1 GPS 37
5.2 AIS 39
6 Conclusion 41
6.1 Future work 42
Bibliography 43
A Appendix 45
A.1 Electronic questionnaire with associated information letter 45

List of Figures

1 Response limit . . . 13
2 Response editing . . . 15
3 Multiple responses . . . 15
4 Anonymous responses . . . 18
5 Question 1 . . . 22
6 Question 2 . . . 23
7 Question 3 . . . 24
8 Question 4 . . . 25
9 Question 5 . . . 26
10 Question 6 . . . 27
11 Question 7 . . . 28
12 Question 8 . . . 30
13 Question 9 . . . 31
14 Question 10 . . . 33
15 Questionnaire page 1 . . . 46
16 Questionnaire page 2 . . . 47
17 Questionnaire page 3 . . . 48
18 Questionnaire page 4 . . . 49
19 Questionnaire page 5 . . . 50
20 Questionnaire page 6 . . . 51

1 Introduction

1.1 Problem Description

The maritime sector is increasingly dependent on digital systems; systems that in many cases was initially designed without security in mind. At the same time, it is reported that the levels of information security awareness within the sector is low to non-existing. It is reported that low levels of information security awareness, and security issues with GNSS and AIS, are among the top 10 digital vulnerabilities within the maritime sector [1]. Low levels of awareness, combined with vulnerabilities in the technical systems, has the potential to make the sector even more vulnerable than if the awareness was high, or the technical systems completely secure. There are several examples of how scientists have proven that the wireless systems can be manipulated, and how. But the lack of high profile incidents has kept the awareness levels at a low level [2]. This thesis aims to uncover the relationship between actual security in GNSS (GPS especially) and AIS, and how the stakeholders within the sector consider it to be. The initial hypothesis is that the considered security is higher than the actual security.

1.2 Research Questions

The problem description can be structured into 2 research questions as follows:

Q1: To what extent are maritime stakeholders aware of security issues in the wireless technologies they utilize?

Q2: To what extent does the maritime stakeholders consider the security issues to be a concern towards safety?

2 Basic concepts and previous work

2.1 GPS (Global Positioning System)

The Norwegian government appointed “Lysne” committee state in their report of 2015 that one of the top 10 digital vulnerabilities in the maritime sector is that the signals from the satellite navigation systems are not protected against modification. GNSS (Global Navigation Satellite System) is a crucial tool when navigating at sea. GPS (Global Positioning System) is the most widespread satellite navigation system around; also in the maritime sector. GPS has several known vulnerabilities. For instance, the civilian part of this system is not protected against malicious modification. This makes it vulnerable to spoofing. It is also inherently susceptible to jamming [1]. This makes it highly vulnerable to DoS (Denial-of-Service) attacks. It would be easy for a passenger to jam the GPS signals by bringing low-tech and low-cost equipment on-board. Of all accidents at sea, 50% are caused by some sort of navigational error (willing/unwilling, human/digital). Navigational errors could have severe consequences, especially when dealing with transportation of passengers or hazardous goods. It could for instance be critical if a supply ship using DPS (Dynamic Positioning System) to “hover” in close proximity to an oil installation, lost their access to trustworthy satellite navigation [1].

2.1.1 Jamming

In a GPS jamming event, a hostile counterpart will block the GPS signals so that the vessel cannot receive them [1]. This is done by using a transmitter to drown the legitimate signal in noise. GPS jamming equipment is easily available, at different prices and ranges. Low-range jammers can be acquired for a couple of thousand NOK, while high-range jammer lies in the 100000,- NOK price range. A low-power jammer of 1 watt mounted on a drone could jam the GPS signals in a radius from 10-85km, depending on if the receiver has signal lock or not. Jammers from the lowest price ranges can be bypassed by the use of reasonably priced filters. To withstand an attack from more advanced jammers on the other hand, would require techniques that are only used for military applications today. A jamming event is quite easy to detect, since the system becomes unavailable, but it will result in a total loss of service. GLA (The General Lighthouse Authorities of the United Kingdom and Ireland) has performed tests to assess the impact of a GPS loss of service. They discovered that a range of other systems were impacted by this [1].

The primary source of PNT (Position, Navigation and Timing) in the maritime sector today is GPS. Both as a stand-alone system, and in combination with others. Being a radio communication technology, GPS is inherently susceptible to jamming. In addition to this, due to great distances, the GPS signals are extremely weak when they reach earth. This makes the system even more vulnerable. With this backdrop, the General Lighthouse Authorities of the United Kingdom and Ireland (GLA) and the UK Ministry of Defence (MOD) conducted a range of research trials to investigate GPS jamming and its impact on the sector. The jamming equipment was provided and operated by MOD scientists. The jammer used was a professional low-to-medium power VHF controlled GPS jammer. In the first trails, a vessel was manoeuvred into the coverage area of the jammer [3].

When the vessel entered the GPS jamming zone, alarms were generated on the bridge. The alarms reported issues with systems like DGPS (Differential GPS) receivers, the AIS (Automatic Identification System) transponder and the DPS. The crew, with their prior knowledge of the trials, was able to tie all these alarms to loss of the GPS service. The report states that a large number of alarms, like in this case, could play out quite differently in a real-life scenario. It could create confusion, and it could take the crew some time to regain control over the situation. During this time period, the crew is very susceptible to making errors. The primary means of navigation onboard the vessel used in these trials was ECIDS (Electronic Chart Display and Information System). When the GPS signals were jammed, ECDIS froze. The secondary means of navigation on board is paper charts. The researchers point out that it might be very difficult for crews around the world to revert back to old fashioned methods, due to the lack of day to day experience with it. It is crucial that the crew is able to detect that the GPS service is gone or untrustworthy. If they do not recognize this, issues with GPS will impact the safety and security gravely. It will also be important that the crew is familiar enough with alternative means of navigation and have the necessary situational awareness. In these trials, the crew was aware of the details of the trail. They knew what to expect, at which time, and how to deal with it. The research performed does not represent an unprepared real-life scenario [3].

GLA is worried about several aspects of the GPS system. Over-reliance on the system, and general GPS vulnerabilities, makes GLA recommend a more redundant system. They point out that vessels should make use of two separate satellite navigation systems, together with land-based solutions like eLoran. The use of two satellite navigation systems mitigate issues with the service, while the use of a land-based technology mitigates GNSS related vulnerabilities for all space systems [3].

The trials did also consist of testing the result of GPS jamming on a range of AtoN (Aids-to-Navigation) services. They observed that eLoran was not affected by the jamming, but that it does disrupt the service provided by the DGPS reference stations. The ship was equipped with three GPS receivers for the occasion. All three of them lost signal lock during the jamming efforts. The receivers supporting DGPS kept signal lock for the DGPS signals; but these could not provide any reference. Among the alarms on the bridge, we find alarms from the AIS (Automatic Identification System) system. Losing GPS render AIS useless [3]. AIS utilize GPS as the timing source, so in a GPS loss of service, AIS will be lost as well [1]. The researchers conclude that a GPS jamming incident, using low-power jammers, will have significant impact on maritime safety [3].

2.1.2 Spoofing

GPS is inherently susceptible to spoofing [4]. While the military version of GPS is hard to spoof; the civilian is not. One reason for this is that the attacker can easily detect how the legitimate GPS signals is seen by the legitimate receiver. With this knowledge, combined with the lack of sender authentication in the system, there is no match for an attacker to design a similar signal, carrying falsified information [4].

Protection against spoofing is only used in military applications of GPS [1]. This is done through the use of encryption [4]. This will make it difficult, if not impossible, for an attacker to know what the legitimate receiver is seeing. In a GPS spoofing attack, the attacker would provide the user with modified navigational data; either by modifying the legitimate signal, or through impersonation. If the navigator does not detect the errors in the data, the modified data could be used to alter course [1]. This has multiple applications. The result could be accidents like collisions or running ashore. Researchers have shown how a GPS spoofing attack at sea could be successfully carried out [1]. In 2013, researchers at the university of Texas brought on board a suit case sized GPS transmitter (purpose built GPS spoofer). They used the transmitter to provide the navigators with false navigational data through the ships GPS receivers. Neither the navigational systems, nor the on-board personnel, was able to detect that the data was fake; and the course was indeed altered. Unlike with a case of loss of service, a spoofing attack will not raise any alarms, as the receiver indeed has signal lock. The lead researcher, Todd Humphreys, said to UT News after, that he had not expected the GPS spoofing to be so easy to perform, and so difficult to detect [5].

In August 2017, the Norwegian industry newspaper for the telecommunication industry, Digi.no, wrote about incidents of GPS spoofing. The mentioned incidents were said to have occurred in June 2017, in the Black Sea. Reportedly, dozens of ships had experienced what was obviously spoofed GPS information. One of the affected ships reported to the US Coast Guard that the GPS systems on board showed them that the vessel was on dry land, when it indeed was not. The alleged spoofing came and went over a period of a couple of days. It is not reported how many vessels in the region that was affected, but it was observed and reported by approximately 20 ships. Not only is it suspected that this was a case of GPS spoofing, but also that it is a result of a test of a Russian GPS spoofing system. Russia has become the main suspect do to geographical location, and that the Russians already are familiar with GPS spoofing. In one recent event in 2016, a GPS spoofer and jammer was detected in the Kreml area. Like others, Digi.no also points to Loran-C and eLoran as backup technology that are practically immune to satellite related issues [6].

2.2 AIS (Automatic Identification System)

As with GPS, the “Lysne” committee also views the lack of protection against signal modification in AIS as one of the top 10 digital vulnerabilities in the maritime sector [1]. AIS is together with GPS, one of the most important wireless technologies used at sea, and is a crucial tool in traffic monitoring and vessel assistance [7]. It is a vessel identification system initially designed to avoid collisions at sea [1]. AIS function by collecting their own spatial parameters through GPS, and transmit these over VHF to other vessels and maritime authorities. The transmitted signal fully identifies the transmitting vessel with a range of parameters, like vessel name, exact position, velocity and course. The data is used for a range of applications, for instance by other vessels to avoid collisions, or by maritime authorities to send out weather forecasts or coordinate SAR (Search and Rescue) missions. Through the notable service called aids-to-navigation (AtoN) the AIS system also provide the vessels with data concerning other objects than vessels. Objects like lighthouses and buoys will transmit information regarding weather conditions, together with their own position. Everyone with an AIS transponder must register. They will then receive an MMSI (Maritime Mobile Service Identity). It is the MMSI that identifies the vessel (or other object), or rather the AIS enabled station, in the system. This is issued by national maritime authorities together with their VHF call sign [7].

Like with GPS, AIS is not designed with security in mind. There is no system in place for authentication, and no encryption [1]. This makes it highly vulnerable to spoofing. Trend Micro performed a security analysis of AIS back in 2014, and the result were discouraging. Using simple equipment, an attacker could exploit a range of serious vulnerabilities [1]. The Trend Micro researchers designed a simple AIS transmitter, and ran simulations to uncover how real equipment would react to spoofing and manipulation of the system. They identified a range of threats that we will discuss in later sections [7].

2.2.1 Ship Spoofing

The act of ship spoofing, as defined by Trend Micro, is the spoofing of a non-existing ship posing as real. To achieve this, the fictional ship is assigned parameters to be distributed though AIS, like vessel name and MMSI. The spoofer will also need to generate and distribute dynamic parameters like position, velocity and course [7].

2.2.2 AtoN Spoofing

In AtoN spoofing, the vessels are provided with manipulated information regarding their surroundings, and tricked into making wrong decisions [7].

2.2.3 Collision Spoofing (CPA)

In collision spoofing, the CPA (Closest point of approach) functionality of the AIS system is manipulated. This is a system that automatically alert in the case of expected or actual collisions. The minimum distance between two vessels are calculated, and the system alerts if this minimum distance is exceeded. If configured, CPA will alert the captain, and automatically alter the course to avoid or minimize impact. In a collision spoofing attack this functionality is triggered on false premises. This technique could be used to alter the vessels course, potentially running it aground or facilitating an actual collision [7].

2.2.4 AIS-SART Spoofing

In AIS-SART spoofing, SARTs (Search and Rescue Transponders) are spoofed to launch search and rescue operations on false premises. When a SART hits water, it triggers a radio beacon containing the GPS position of the device. In an attack, the attacker could transmit a false distress beacon for a man overboard, containing GPS coordinates chosen by the attacker. Nearby AIS devices will alert upon this beacon, and the receiving vessel is obligated to assist, together with the authorities. This technique could be used to lure vessels into hostile waters [7].

2.2.5 Weather Forecasting

AIS is used for weather forecasting purposes through received information about dynamic environment parameters. If an attacker were to manipulate this data, the crew could be thinking they were in for a sunny day when they in reality were heading into a storm; and vice versa [7].

2.2.6 AIS Hijacking

In AIS hijacking, the attacker intercepts and modify AIS traffic carrying parameters about the specific AIS station (e.g. course, velocity, GPS position). This could be achieved by transiting a false AIS signal overpowering the legitimate signal [7].

2.2.7 Availability Disruption Threats

An AIS availability disruption would be the AIS equivalent of a DoS attack. Trend Micro divides the threats into three categories. The first category is slot starvation. Here, the attacker impersonates maritime authorities to be able to occupy the full width of the AIS address space. This will prevent all AIS stations within the area from using the system. This includes vessels and AtoN devices. The second category is what Trend Micro has chosen to call frequency hopping [7]. This must not be confused with frequency hopping as a wireless communication security technique. In an AIS frequency hopping attack, the attacker will again impersonate maritime authorities. This time they will force the AIS stations in the area to change frequencies, and thereby making the station useless. This cannot be overridden by the vessel. The last threat described is called the timing attack. In an AIS timing attack, the attacker instructs an AIS station to delay its transmission. This can in principle be renewed indefinitely, and keep the station offline. The vessel will not be able to distribute their parameters, and go off the grid. The attacker could also flood the system by forcing stations to distribute their parameters at a very high rate [7].

2.2.8 The Experiments

The experiments performed by Trend Micro were carried out in a lab to avoid interfering with live services, using an AIS transmitter as the attacker, and an AIS receiver as the victim. Several different receivers were used to make sure that the vulnerabilities were not brand specific. For message generating and transmitting, the researchers used a purposes built, GnuRadio based AIS transmitter which they named AISTX [7]. Being a GnuRadio based SDR (Software Defined Radio) device, makes it low cost, and with very little hardware involved. This means that an attacker could bypass the expenses related to, and most importantly, the difficulties of obtaining, suitable RF hardware. Being purpose built also means that the attacker can generate any AIS system message at will.

Using the AISTX, they observed on their receivers that they successfully posed as a fictional Italian vessel called “FOO”, with MMSI, velocity and GPS position of choice. They also applied this methodology to pose as a range of other crafts, e.g. military vessels, law enforcement, freighters carrying dangerous cargo, AtoN buoys and SAR aircraft [7].

To simulate collision spoofing, they spoofed a fictional vessel, and set it on a collision course with the AIS transponders in the lab. The necessary parameters were derived from the AIS information distributed by the victim. The spoofed ship is then configured to appear within the CPA threshold of the victim. They successfully triggered a collision alarm in the victim equipment, with an expected impact in 6 meters and 2 seconds [7].

The researchers were also able to create and transmit malicious weather forecasts, that was correctly interpreted by the AIS transponders. All AIS transponders are required to trigger a SAR alarm when it picks up on a distress beacon. To achieve this, the team emulated an AIS-SART transmitter, and transmitted a distress beacon [7].

Up until now we have looked at instances of impersonation and spoofing. The next main block in the Trend Micro research goes into what they have called AIS hijacking. In an AIS hijacking attack in the RF domain, the attacker overrides the legitimate transmitter's AIS transmission by overpowering it whit its own. In practice, the attacker will transmit a signal with more power than the legitimate signal. The other AIS transponders will not be able to detect the legitimate signal, but will receive the signal of the attacker. The attacker can now insert the parameters he desires, and this will be detected by the surrounding AIS transponders. This was successfully achieved in the lab tests [7].

Then the researchers went on to have a look at what they have called availability disruption. To achieve this, they made use of AIS control messages that are reserved by the maritime authorities. First, they tried out the frequency hopping attack. Here they transmitted a control message instructing the receiving AIS transponder to move to a non-standard operating frequency. This successfully prevented the AIS transponder from both transmitting and receiving parameters [7].

The timing attack is performed in a similar fashion. Again, using control messages, they instructed an AIS transponder to delay their transmission by 15 minutes. By repeating this, an attacker can keep an AIS transponder "off the grid" for as long as he desire, making it a DoS attack [7].

In the last experiment, they launched a slot starvation attack. In this attack, they used control messages to allocate all TDMA slots to themselves. Effectively leaving no available slots for other AIS transponders. This will prevent them from both transmitting and receiving [7].

The real-life application of the findings where tested by transmitting harmless test messages form the AISTX to an AIS transponder mounted on a moving vehicle. The tests were successful [7].

2.3 Similar projects

There has not been performed any studies on this issue in the maritime sector, but Strohmeier et al. have recently published an article on this issue in regards to aviation. In their article "On Perception and Reality in Wireless Air Traffic Communication Security" they compare the actual security of wireless air traffic communication technologies to how secure the individuals within the sector consider them to be [8]. In other terms; they are measuring the level of awareness in the sector on this specific matter. They state that the inherent vulnerabilities of these wireless communication technologies have been uncovered and exploited by security professionals to demonstrate attacks, but that this have not "resonated widely" within the sector. Therefore, they hypothesize that either the vulnerabilities in these systems are widely known throughout the sector, but not thought exploitable; or they are not known at all. Their investigation shows that are indeed a grave mismatch between the research in the field and the approach of the sector. It is uncovered that the surveyed aviation professionals are indeed unaware of the security issues with these technologies [8]. This article has proven a great inspiration in the process of designing the initial problem description and questionnaire of this thesis.

3 The survey

This thesis will include two main components: A theoretical component, and an empirical component. The analysis of the wireless systems will be briefly analysed using existing literature. The review will not be exhaustive, but a range of vulnerabilities discovered and exploited by researchers will be described and discussed. To measure the awareness, a survey will be used as the strategy. A questionnaire will be used as the data generation method. The data from the questionnaire will be analysed using qualitative data analysis.

3.1 Survey

The basic idea of a survey is that you can apply your findings to a larger population than the one you actually surveyed. This is done through the use of statistical methods [9]. The survey in this thesis could aim to be representative for the surveyed group so that the findings could be used to look for patterns and generalization for the whole community, but only if the number of respondents allow it. If the number of respondents are too low for the results to be applied to the whole community, the results can be used to look at some trends and traits, using a qualitative data analysis. That is what we will do in this thesis.

Oates break the survey strategy into six different activities: Data requirements, data generation method, sampling frame, sampling technique, response rate and non-responses, and sample size [9].

3.1.1 Data requirements

Data requirements are the requirements concerning what kind of data you want to generate. It can be separate into two categories: Directly topic related, and indirectly topic related. In regards to this thesis, how secure you assess a certain wireless system to be would be considered to be directly topic related. Your position category and level of education, would be considered indirectly topic related [9].

3.1.2 Data generation method

The data generation methods deals with how the data is generated/collected. In this thesis, we are interested in obtaining pre-defined answers to a range of identical questions. Therefore, a questionnaire will be used as the data generation method. The design of the questionnaire will be discussed in a later section.

3.1.3 Sampling frame

A sampling frame describes the population that could be included in the selection. I.e. the population you wish to apply your findings to [9]. Since the research questions deals with the maritime sector, the whole sector is considered to be the sampling frame. It is from the maritime sector that the selection will be made.

3.1.4 Sampling technique

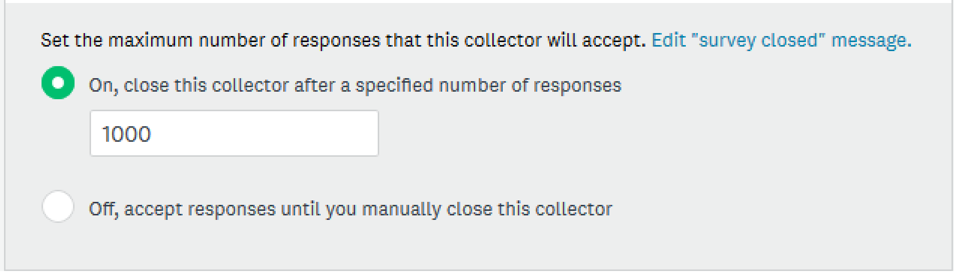
The sampling technique deals with how the selection of respondents (in this case) is made. In more general terms: How to select people from the sampling frame. There are two kinds of sampling: probability sampling, and non-probability sampling. In probability sampling, there is a high probability that the selection is representative for the whole population. In non-probability sampling this link is not known. This means that you cannot apply the findings to the whole population, but only use the data as indications [9]. Since we are going make use of a qualitative data analysis, we will make use of non-probability sampling. SINTEF will use their professional network in the maritime sector to help with gathering a sufficient number of respondents. This approach is often called convenience sampling. In convenience sampling, the respondents are selected simply because they are available [9]. It is of course crucial that all of the respondents are members of the maritime sector for the research to be of any value.

3.1.5 Response rate and non-responses

Response rates of approximately 10% is not uncommon with questionnaires [9]. To increase the number of respondents, SINTEF will provide indirect access to their professional network in the maritime sector.

3.1.6 Sample size

To be able to decide on the sample size, several aspects must be taken into account. The response rate will be important. How many actual respondents are you likely to get? It will also be important to know how many respondents you need for the survey to be representative for the population [9]. The Norwegian maritime sector employs approximately 100000 people [10]. For a survey of a population of 100000 people to have a 95 per cent confidence level and a +/- 3% accuracy range, we would need 888 respondents [9]. This is not feasible for a 30-credit master's thesis. A sample size of approximately 200 respondents are more feasible. This means that we would have trouble applying the results to the whole population using a quantitative data analysis. This does not mean that we cannot use the collected data to look for trends. This will be discussed later in the thesis. Due to financial considerations, the maximum response limit for this survey will be set to 1000 respondents. This can be set in the service provider's design tool as seen in figure 1.



Set the maximum number of responses that this collector will accept. Edit "survey closed" message.

● On, close this collector after a specified number of responses

1000

○ Off, accept responses until you manually close this collector

Figure 1: Response limit setting in SurveyMonkey.

SurveyMonkey also provide some guidelines as to how to calculate the necessary number of respondents. The initial rule of thumb is that the more confident you want to be in your results, the more respondents you need [11]. Getting a sufficient number of respondents has proven to be a difficult task for many theses, so calculating a minimum threshold for the number of respondents would be useful. SurveyMonkey provide us with a sample size calculator [12]. The definitions and algorithms implemented in this is fully explained [11]. Our population size is 100000. If we set our confidence level to 95%, and the accuracy range/margin of error to +/- 15%, the calculator gives us a suggested sample size of 31 respondents. In cooperation with the supervisors, the minimum number of respondents for this survey was set to 30. This would not be enough for a full quantitative analysis, but it would enable us to look at some trends and traits with a more qualitative analysis.

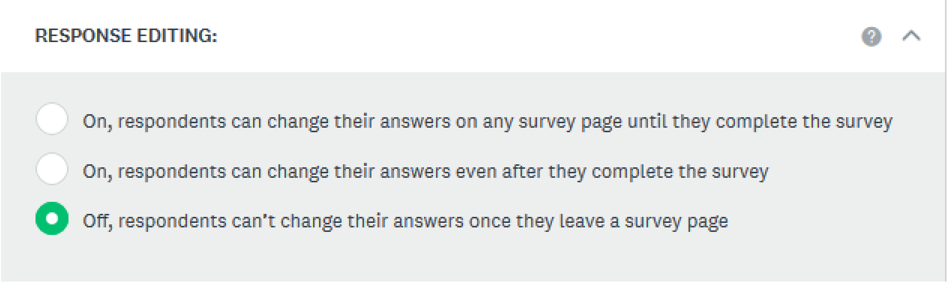
3.2 Questionnaire

Questionnaires are a very commonly used data generation method with the survey strategy, and is well suited for this thesis as well. The questionnaire will be a self-administered, internet based questionnaire using the service provider SurveyMonkey. A self-administered questionnaire is a questionnaire that is completed by the respondent without the researcher being present [9]. This is the best solution in regards to this thesis, since it allows for a large number of respondents with little time consumption. It cannot be justified to tie up the necessary hours to administer the questionnaires personally with the thesis being only 30 credits.

In previous sections, we talked about directly topic related and indirectly topic related. Using a questionnaire, we distinguish between two types of questions in regards to what kind of data you want to generate: Factual data, and opinions.

Factual data could be job title or date of birth; while opinions could be what the respondent thinks about a certain information system. You can collect both kinds of data using the same questionnaire, but it is important to keep in mind what kind of data you want to collect when designing the question [9]. The questionnaire in this thesis will collect both kinds of data. A questionnaire also distinguishes between open and closed questions. In an open question, it is completely up to the respondent to figure out the answer using a blank field. In a closed question, the respondent is forced to choose from a range of pre-defined answers [9]. The questionnaire used in this thesis will make use of closed questions, for a more quantified result. We are more concerned with the general trends of the sector, than very specific opinions of individuals within the community. It would also require substantially more time and effort to code and analyse an open question questionnaire [9].

It is also important to consider the format of questions and responses. There are many forms, yes/no and agree/disagree being among them [9]. For this thesis, we will use scale questions for gathering the opinions. In a scale question, the respondent is provided with a statement, and is asked to tick the box on a scale that matched their views most closely. In the example provided by Oates the respondent is given a statement, and is asked to tick a box on a scale saying either “about right”, “good”, “bad”, “very good”, or “very bad” [9]. Several choices has been made in the creation of the questionnaire. In regards to practical considerations, we have chosen to not introduce the concepts of GPS and AIS to the respondents. This to avoid colouring of their genuine opinions. The logic is that if the respondent is introduced to the GPS technology in a way that highlight its importance, this can affect the actual response. It has also been made impossible to manoeuvre back to previous questions, for much the same reason. We want to capture the genuine awareness of the respondent as untainted as possible, and don’t want the answers to be coloured by realizations made during the questionnaire process. In practice, this is done through the deactivation of “response editing” in the collector, as shown in figure 2.



RESPONSE EDITING:

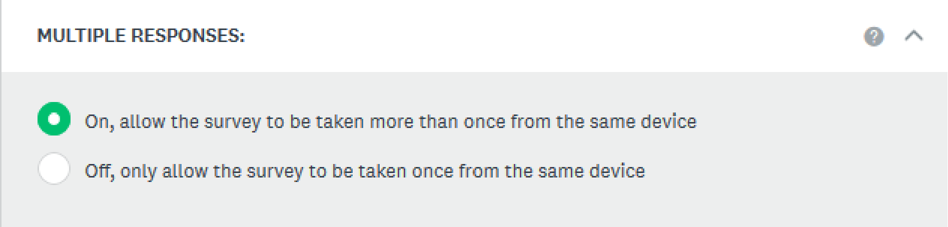
○ On, respondents can change their answers on any survey page until they complete the survey

○ On, respondents can change their answers even after they complete the survey

● Off, respondents can't change their answers once they leave a survey page

Figure 2: Response editing setting in SurveyMonkey.

We have also allowed that the electronic questionnaire can be filled out more than once from the same device. This is done so that multiple respondents can use a shared computer (e.g. common computer on a vessel). This function was activated as shown in figure 3.



MULTIPLE RESPONSES:

● On, allow the survey to be taken more than once from the same device

○ Off, only allow the survey to be taken once from the same device

Figure 3: Multiple responses setting in SurveyMonkey.

In addition, we have chosen to bold out key terms, like GPS and AIS. This is done to insure that the respondent is certain about which technology he or she is dealing with at the moment.

We have also chosen to make all the multiple choice questions mandatory, because all of the questions are considered crucial to the thesis. We have also added textboxes at the end of the questions that measure opinions. These textboxes are included for any calcifications the respondent wish to make. The textboxes are not made mandatory, since they are not crucial to the analysis (especially if the respondent does not have to, or want to, make any clarifications). The effort has also been made to keep the questions as clear and concise as possible, without them losing their essence. They are designed in a way that we think is the best way to avoid confusion and room for interpretation. We have also tried to avoid discipline specific terms to the information security field. This because the majority of respondents typically won't be information security professionals. For the least tech-savvy of the respondents, we have also included a “I don’t know” option for the opinion questions.

It will also be important to provide the potential respondents with information reassuring them that their responses will be kept confidential, and the completion of the questionnaire itself is completely voluntary. Clear instructions are also important [9]. All this will be included at the beginning of questionnaire. The questions should be grouped together after topic to ensure internal logic [9]. In the questionnaire used in this thesis, the factual data will be collected in the beginning, and the opinions will be collected in the end. The actual questionnaire can be found in the appendix of this thesis.

3.3 Research ethics

When doing research, it is important to be ethical. That is, to treat every involved party fairly and with honesty [9]. Like any other project, this project has parties. Both the author of the thesis, the supervisors, the academic institution, SINTEF, the authors of research and other literature used in the thesis, and copyright holders, are parties. This comes in addition to the respondents of the electronic questionnaire.

Academic honesty is crucial. A basic principle when using research done by others, is to reference their work correctly. Not referencing it correctly implies that you present it as your own work. That is not acceptable, and is considered as plagiarism [9]. It is also crucial to ensure that you have the right to use copyrighted material, e.g. images and other visual elements.

The data gathering using this questionnaire is reported to The Data Protection Official for Research. This is mandatory for all data gathering concerning personal data. The electronic questionnaire will be distributed through the use of a web link, and are therefore avoiding the logging of e-mail addresses. The IP addresses of the respondents will be known to the service provider when they are responding to the questionnaire, but they will not be logged. Informed and active consent is ensured by the use of electronic questionnaires. A completed electronic questionnaire is legally valid as active consent.

The respondents of the electronic questionnaire have certain rights. They have the right not to participate, the right to withdraw, the right to give informed consent, the right to anonymity, and the right to confidentiality [9]. The participants in this project will receive a written information letter describing the project and the questionnaire. The letter can be found in the appendix, as the introduction to the questionnaire.

3.3.1 Right not to participate

The right not to participate is an important principle in ethical research. Participation in this study, through the electronic questionnaire will be on a completely voluntary basis.

3.3.2 Right to withdraw

The right to withdraw from the project ensures that a participant can pull out if questions they do not want to answer emerges, or they do not feel comfortable with certain activities. This aspect is quite easy to ensure when using anonymized electronic questionnaires as the data generation method. If the respondent is uncomfortable with any of the questions, or some other aspect of the activity, he or she would simply not complete the electronic questionnaire. This is perfectly okay, even if they were initially positive towards participating.

3.3.3 Right to give informed consent

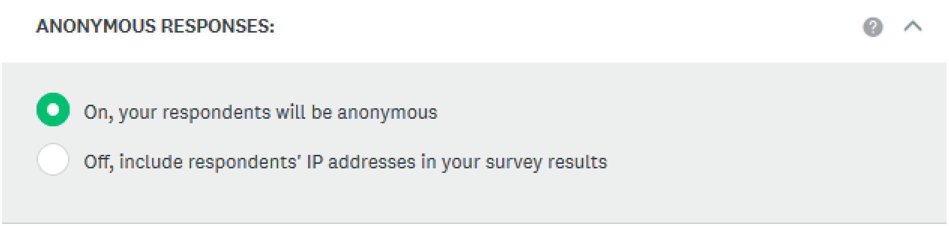
The participants of a research project has to give consent. It is also an important ethical aspect that the consent is informed. This means that the participants are informed about the nature of the research and their own involvement. The participants should be informed about [9]:

- The purpose of the research. Why is the research being performed, and what is expected to come out of it?
- Who is performing the research. Name and contact details of the researcher, and details of supervising organizations.
- What the involvement will include (e.g. questionnaire) and how long it will take.
- If they will receive any expenses, payment or other incentive.
- How the researcher will make use of the collected data, and how the results will be disseminated.

The participants of this research project will be informed through a written information letter provided by the author. This letter will account for all the aspects mentioned above. It will also include all the other rights listed in this, and surrounding subsections. The actual consent is given by completing the electronic questionnaire.

3.3.4 Right to anonymity and confidentiality

The participants have the right to anonymity, and the right to confidentiality. [9]. In this project, anonymous response using a web link to the electronic questionnaire will insure anonymity. The service provider will not log the IP addresses of the respondents. When designing the online questionnaire, this is a feature that will be activated; as shown in figure 4.



ANONYMOUS RESPONSES:

● On, your respondents will be anonymous

○ Off, include respondents' IP addresses in your survey results

Figure 4: Anonymous responses setting in SurveyMonkey.

The participants also have the right to confidentiality. This means that the data you gather from them are kept confidential [9]. In this project, the data will be 100% anonymized to the author. The service provider make use of https to ensure the confidentiality during the completion of the questionnaire. All data will be deleted after the completion of the thesis.

3.4 Analysis

As mentioned in earlier sections, the survey strategy will be used in this thesis, using questionnaire as the data generation method. The data will be analysed using qualitative data analysis. Qualitative data is characterised by being non-numeric [9]. A survey/questionnaire approach could very well be analysed using quantitative data analysis, but that would require highly quantified data and a large number of respondents.

The matter of data analysis is seldom a black and white issue; either quantitative or qualitative. Often, we will see that the data analysis is something in between. This is also the case in this thesis. The analysis of the literature will be purely qualitative, as qualitative data will be used to establish if the systems can be viewed as relatively secure or relatively vulnerable. In the second step of the analysis, a combination of the two will be used. The results from the questionnaire (as presented in the results chapter) will indeed be analysed in a quantitative fashion, e.g. by determining the distribution between the answers. But the number of respondents will most likely not be sufficient to perform a satisfactory quantitative analysis where the results can be applied to the whole population. Instead, we will use a hybrid data analysis, where we apply the basic quantitative techniques to the quantified results, but we analyse it in a more qualitative way to be able to extract some trends and indications from the data despite the relatively low number of respondents.

4 Results

4.1 Distribution

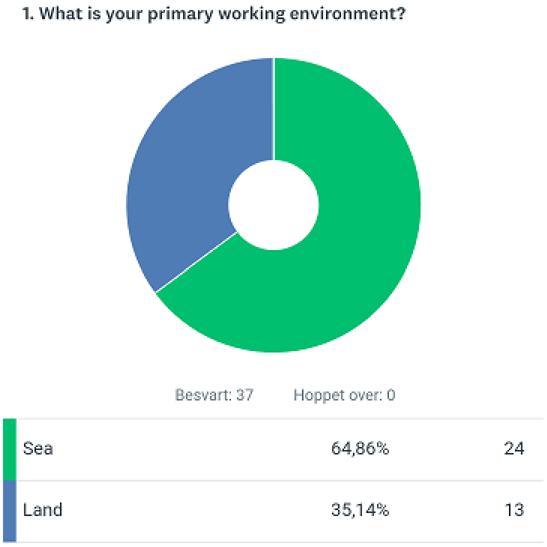
The electronic questionnaire was distributed through a range of different mediums. It was put up on 3 different maritime discussion forums and in 3 different maritime LinkedIn groups. It was also distributed into SINTEF's professional maritime network. A range of shipowners and organizations were asked, but of the few that replied, only the Norwegian Shipowners' Association was willing to participate. They distributed the questionnaire to their member mass by the means of a members only internet article.

4.2 Data

The minimum number of respondents was set to 30 in the initial research design. Getting respondents tends to be a difficult task, and the work with this thesis was not any different. The results from the electronic questionnaire was therefore extracted as soon as we reached 30 complete responses. At the time of data extraction, we had 37 respondents, where 30 complete the questionnaire. That gives us a completion rate of 81%.

4.2.1 Factual data

Question 1-4 is factual data. The full questionnaire can be seen in the appendix.



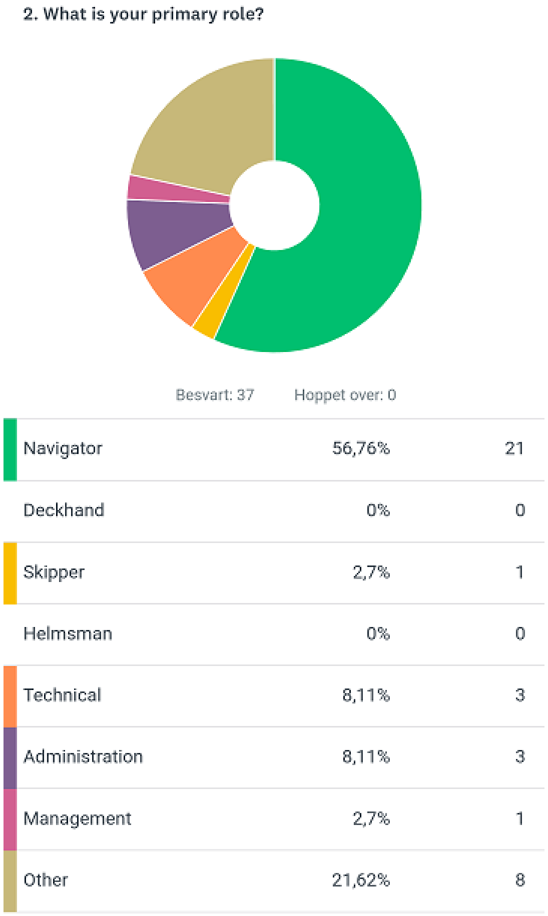
1. What is your primary working environment?

Besvart: 37 Hoppet over: 0

🟩	Sea	64,86%	24
🟦	Land	35,14%	13

Figure 5: Graphic of responses to question 1 of the questionnaire.

As we can see from the figure on question 1, we have 64.86% sea based respondents, and 35.14% land based respondents.



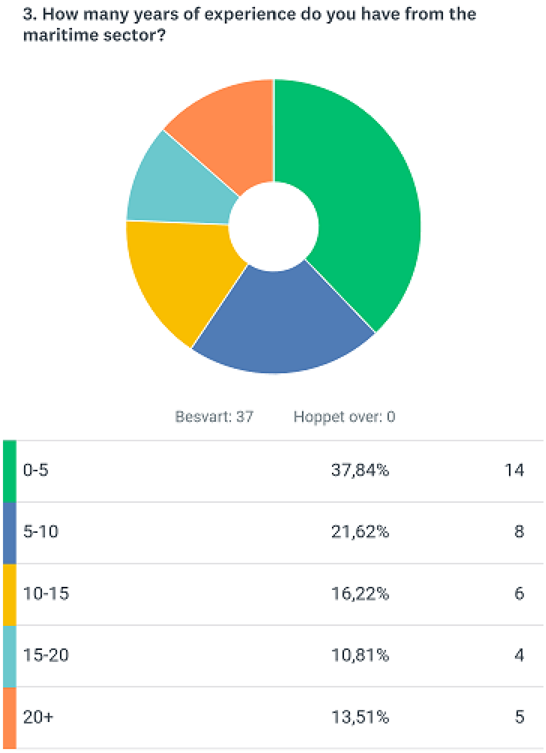
2. What is your primary role?

Besvart: 37 Hoppet over: 0

🟩	Navigator	56,76%	21
	Deckhand	0%	0
🟨	Skipper	2,7%	1
	Helmsman	0%	0
🟧	Technical	8,11%	3
🟪	Administration	8,11%	3
🟥	Management	2,7%	1
🟫	Other	21,62%	8

Figure 6: Graphic of responses to question 2 of the questionnaire.

As we can see from the figure on question 2, we have a large block of navigators, on 56.76%. 2.7% skippers, 8.11% technical, 8.11% administration, 2.7% management, and 21.62% other.



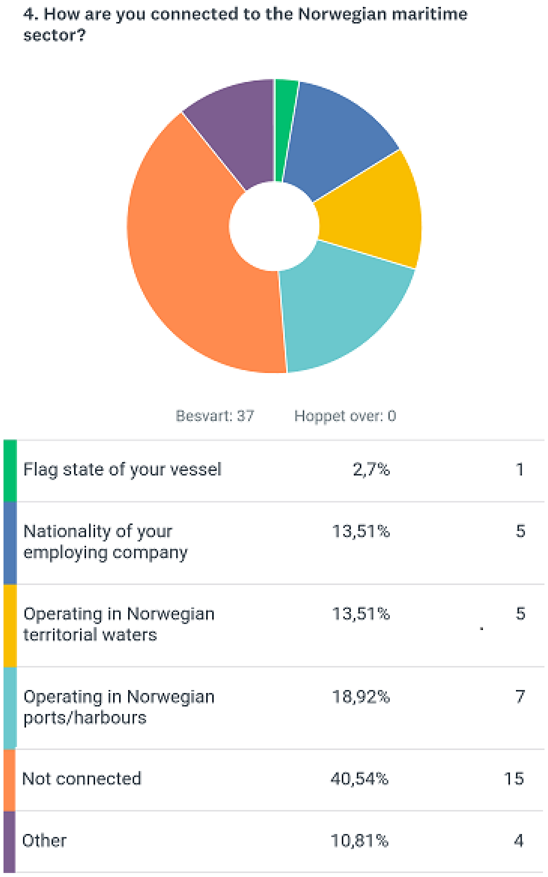
3. How many years of experience do you have from the maritime sector?

Besvart: 37 Hoppet over: 0

🟩	0-5	37,84%	14
🟦	5-10	21,62%	8
🟨	10-15	16,22%	6
🟦	15-20	10,81%	4
🟧	20+	13,51%	5

Figure 7: Graphic of responses to question 3 of the questionnaire.

On question 3 we have a good ratio between the different levels of experience. 0-5 years at 37.84%, 5-10 years at 21.62%, 10-15 years at 16.22%, 15-20 years at 10.81% and 20+ years at 13.51%.



4. How are you connected to the Norwegian maritime sector?

Besvart: 37 Hoppet over: 0

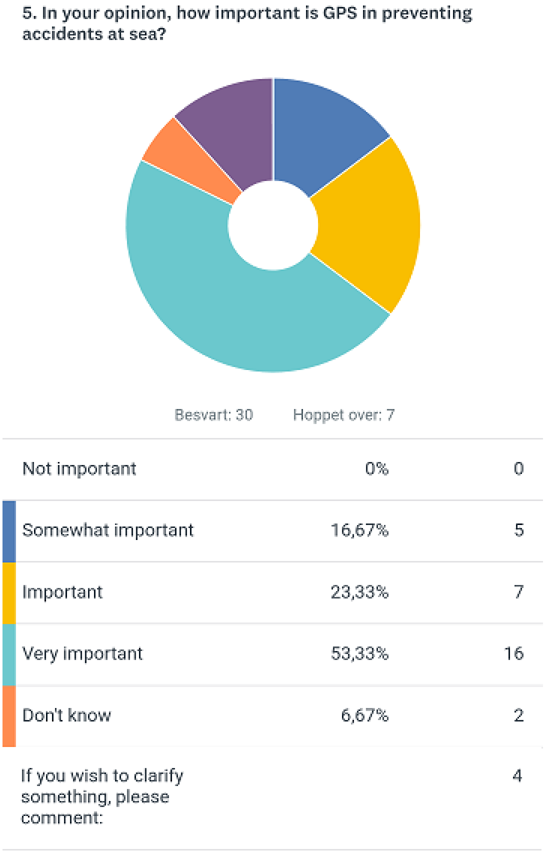
🟩	Flag state of your vessel	2,7%	1
🟦	Nationality of your employing company	13,51%	5
🟨	Operating in Norwegian territorial waters	13,51%	5
🟦	Operating in Norwegian ports/harbours	18,92%	7
🟧	Not connected	40,54%	15
🟪	Other	10,81%	4

Figure 8: Graphic of responses to question 4 of the questionnaire.

On question 4 we see that we have a good ratio between personnel that are connected to the Norwegian industry, and personnel that are not. With 40.54% of the respondents not connected to the Norwegian industry in any way, it leaves us with 59.46% that are connected.

4.2.2 Opinions

Question 5-12 is opinions. Here we will only present the graphics, and render the comments made by the respondents. The comments are rendered as typed by the respondents, with no modification. Some of the comments made are clearly related to previous comments, but it has not been made any effort to link them together in this thesis.



5. In your opinion, how important is GPS in preventing accidents at sea?

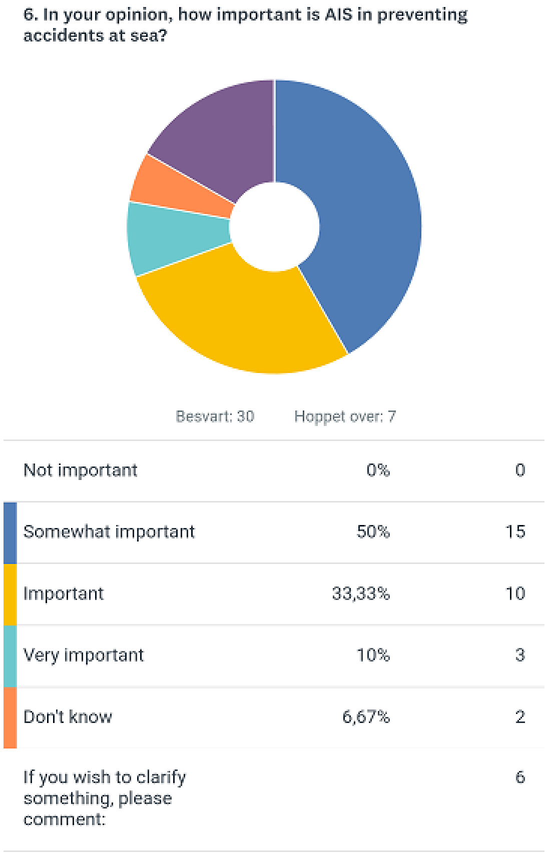
Besvart: 30   Hoppet over: 7

Not important	0%	0
🟦 Somewhat important	16,67%	5
🟨 Important	23,33%	7
🟩 Very important	53,33%	16
🟧 Don't know	6,67%	2
If you wish to clarify something, please comment:		4

Figure 9: Graphic of responses to question 5 of the questionnaire.

Comments made on question 5:

> "Reduce workload of navigator massively"
>
> "It would not be possible to navigate without GPS today because paperwork has been increased and officer numbers reduced to bare minimum."
>
> "Navigators must use all available means to avoid collision, GPS is not important, it is just one of the many tools."
>
> "Very important, however it cannot be relied on whilst deep sea, as satellite connection may be lost during bad weather i.e. fog."



6. In your opinion, how important is AIS in preventing accidents at sea?

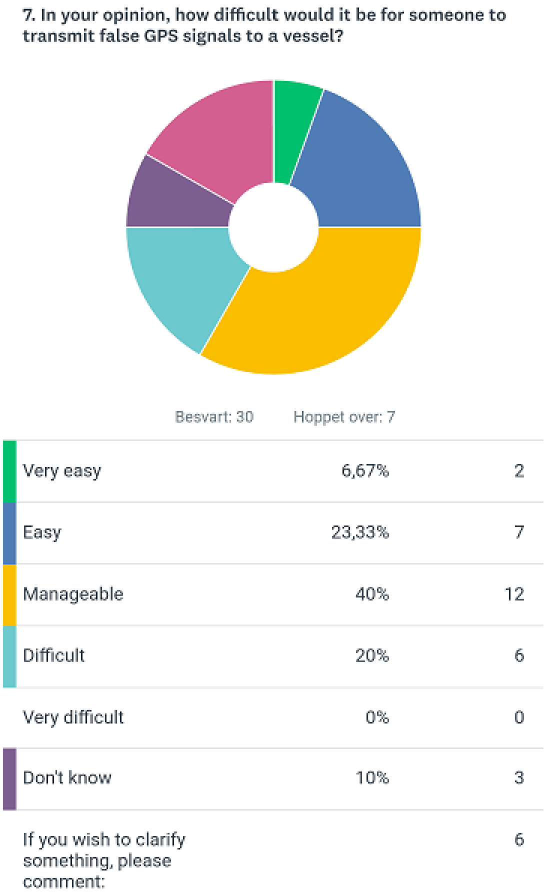
Besvart: 30 Hoppet over: 7

Not important	0%	0
Somewhat important	50%	15
Important	33,33%	10
Very important	10%	3
Don't know	6,67%	2
If you wish to clarify something, please comment:		6

Figure 10: Graphic of responses to question 6 of the questionnaire.

Comments made on question 6:

> "AIS is an information service NOT a collision avoidance device"
>
> "Helps give an idea of destination port so you can anticipate how a vessel will manoeuvre."
>
> "It can help but it can also cause accidents if you call the wrong vessel and arrange a manoeuvre then the vessel you thought you had called sails into your path."
>
> "Helps to positively identify targets. However it is defenitly the cause of accidents when poor OOW's use it for collision avoidence"
>
> "Very important in both open seas and in ports and harbours, as well as Traffic Seperation Schemes."
>
> "AIS is not reliable, will be secondary sensor after radar or visual"



7. In your opinion, how difficult would it be for someone to transmit false GPS signals to a vessel?

Besvart: 30 Hoppet over: 7

🟩	Very easy	6,67%	2
🟦	Easy	23,33%	7
🟨	Manageable	40%	12
🟦	Difficult	20%	6
	Very difficult	0%	0
🟪	Don't know	10%	3
	If you wish to clarify something, please comment:		6

Figure 11: Graphic of responses to question 7 of the questionnaire.

Comments made on question 7:

“I believe it can and has been done but not much vessel crew can do.”

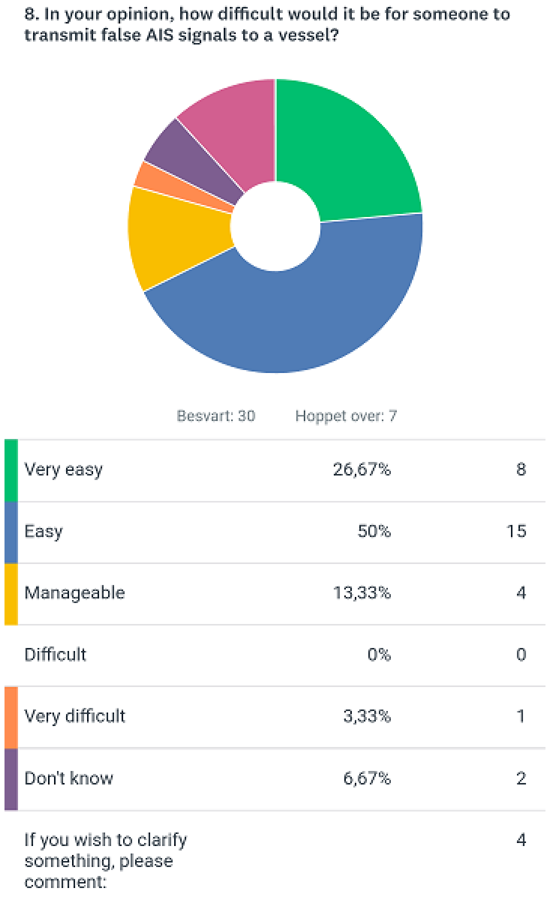
“Blocking would be very easy "spoofing" would be extremely difficult I think.”

“Not at all difficult to block the signal, but for someone to swap my gps signal for their own without me noticing would take a bit of work”

“Depends if the person has the right knowledge in doing such a thing. This may come from a crew member who, may be at first posing as a genuine crew member, but is secretly working for a proscribed organisation, which is highly illegal.”

“Easy for a nation state, hard for the individual. Likely to happen close to shore where GPS is not the primary position fixing method (or shouldn’t be) and not used for collision avoidance.”

“One-off is possible, but long term uphold of false signals will be challenging”



8. In your opinion, how difficult would it be for someone to transmit false AIS signals to a vessel?

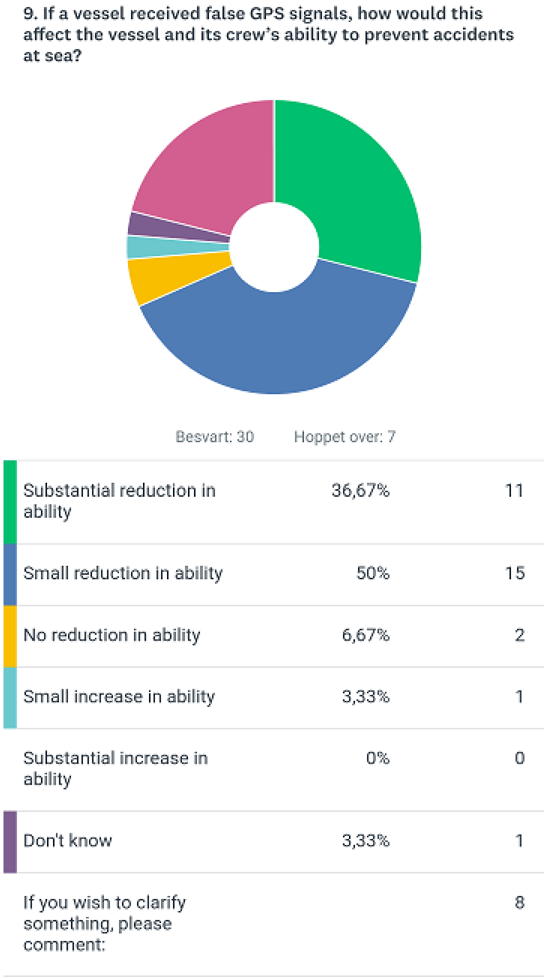
Besvart: 30 Hoppet over: 7

🟩	Very easy	26,67%	8
🟦	Easy	50%	15
🟨	Manageable	13,33%	4
	Difficult	0%	0
🟧	Very difficult	3,33%	1
🟪	Don't know	6,67%	2
	If you wish to clarify something, please comment:		4

Figure 12: Graphic of responses to question 8 of the questionnaire.

Comments made on question 8:

> “This would be corrected by a coast station rather quickly though.”
>
> “Extreamly easy. just need to be within VHF range. so 50 miles at sea level and via satalite”
>
> “Quite difficult, unless someone had the time and willingness to alter the details emmitted by the AIS transponder. I.e. plugging in a laptop to the unit and using the laptop to programme it’s false location to other vessels in the area, which could also cause a collision in the area.”
>
> “However, as AIS is secondary - not so critical”



9. If a vessel received false GPS signals, how would this affect the vessel and its crew's ability to prevent accidents at sea?

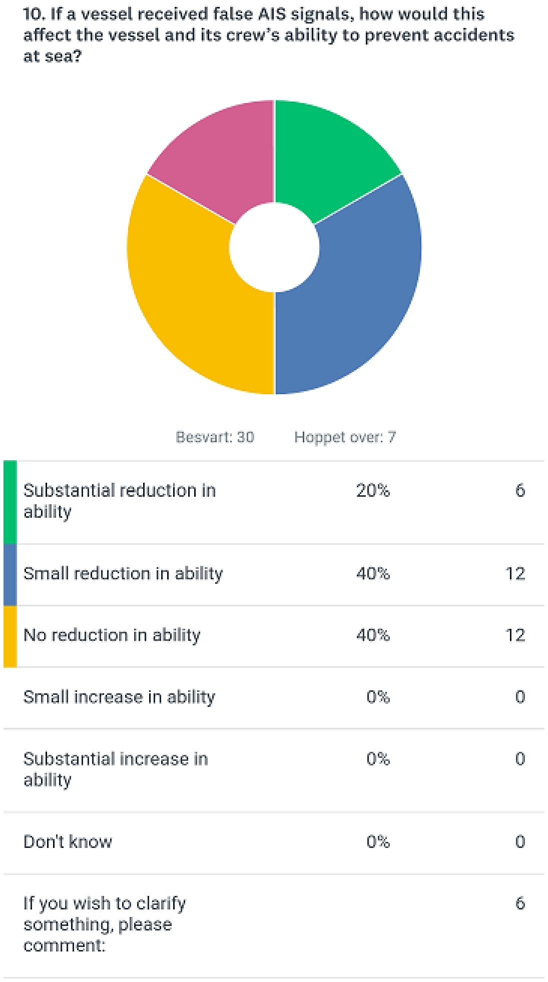
Besvart: 30 Hoppet over: 7

🟩	Substantial reduction in ability	36,67%	11
🟦	Small reduction in ability	50%	15
🟨	No reduction in ability	6,67%	2
▨	Small increase in ability	3,33%	1
	Substantial increase in ability	0%	0
🟪	Don't know	3,33%	1
	If you wish to clarify something, please comment:		8

Figure 13: Graphic of responses to question 9 of the questionnaire.

Comments made on question 9:

> "Depends upon the skill/vigilance of the OOW"
>
> "It depends if crew is using other means, as prudent navigators, other than GPS to determine their position."
>
> "It would depend on whether they realised it or not."
>
> "It would depend on the skill level and experience of the bridge team and how much they relied on GPS compared to visual observation"
>
> "Crews are not accustomed to navigating without GPS."
>
> "Could easily run a vessel aground or even cause a colision if the OOW doesn't notice"
>
> "Crew not able to gaurentee their position unless they could check their position manually and increase watches, and may not be aware of their incorrect position due to latency and not knowing errors."
>
> "OOW is required to keep outlook and check other instruments: Difficult to fool for long time"



10. If a vessel received false AIS signals, how would this affect the vessel and its crew's ability to prevent accidents at sea?

Besvart: 30 Hoppet over: 7

🟩	Substantial reduction in ability	20%	6
🟦	Small reduction in ability	40%	12
🟨	No reduction in ability	40%	12
	Small increase in ability	0%	0
	Substantial increase in ability	0%	0
	Don't know	0%	0
	If you wish to clarify something, please comment:		6

Figure 14: Graphic of responses to question 10 of the questionnaire.

Comments made on question 10:

> "They should be acquiring and monitoring targets visually and electronically outside of AIS"

> "Same comment as q9."

> "As above, but generally bridge teams tend to rely less on AIS info than ARPA / GPS"

> "Unless it happened when the bridge team called another vessel to arrange a manoeuvre and the ais identities had been swapped."

> "A pirate or naval vessel could disguise itself to get close. i cant see it being a cause of an accident. However Someone could spam the ecdis ais overlay and cover important stuff. or could put fake targets in my path to give lots of alarms which would make an oow start to ignore alarms on the brigde"

> "Will normally be correlated to RADAR signals so difficult to see any important impact for normal navigation"

Question 11 and 12 are comments only. Question 11 is as follows: "Do you know any countermeasures that can be used to mitigate attacks using false GPS signals? If yes, please specify below".

Comments made on question 11:

> "Using other methods of navigation. Other e-navigation tools such as E-Loran should be developed as a back up"

> "Not from an electronic point of view. As stated above if proper navigational watch is being maintained other means of position fixing should be used."

> "Coded gps transmission where the ship only received a position based on a coded transmission request, therefore harder to hack..."

> "no"

> "Course alarms / common sense"

> "Good watchkeeping practices. On my previous vessel we had separate brands for the two gps receivers. if there was an actual fault and issue with the signal they would both alarm and I would know not to trust it, if it were a fault with the receiver only one would alarm"

> "Celestial Nav, regular cross-checks."

> "Having someone with IT experience onboard, and also working with coastguards, VTS services and also working with other vessels in the area to conduct periodical GPS signal and position confirmations."

> “Using other position fixing methods to verify/cross check.”
>
> “Use inertial navigation system to verify short term GNSS changes (integrate speed, gyro to estimate new position). More advanced IN systems can be envisaged. One can also use celestial navigation, but that is probably overdoing it. NOTE: This double check is not automated today (ref. grounding of Royal Majesty).”
>
> “Signal strength detection. Radar and visual confirmations.”
>
> “verfied sender, encrypted signals”
>
> “GPS receiver should detect increase in signal strength. Hence integrity data should help detecting.”

Question 12 is identical to question 11, but focus on AIS.
Comments made on question 12:

> “OOWs being able to identify false AIS targets”
>
> “No. See items 6, 10 and 11 above.”
>
> “Same as q11.”
>
> “no”
>
> “Radar”
>
> “Turning it off.”
>
> “Look out of the bridge window?”
>
> “None”
>
> “AIS will normally only be used to give identity to targets identified by RADAR. If in doubt, call ship on VHF. Normally, the actual identity does not matter much. AIS "around corners" are probably not much used.”
>
> “Radar and visual confirmations.”
>
> “verfied sender, encrypted signals”
>
> “Combination of using eyes and radar should help detecting.”

5 Analysis and Discussion

In this section we will compare the data collected through the survey with the examined literature.

5.1 GPS

As we can see in figure 9 in the results section, over 50% of the respondents think that GPS is very important in preventing accidents at sea, while a little over 23% find it important. Some of the comments also reflect this. One respondent say: “Reduced workload of navigator massively”. Another respondent say: “It would not be possible to navigate without GPS today because paperwork has been increased and officer numbers reduced to bare minimum.”. These comments both confirms that GPS is considered important, and also that rationalization plays a part in it. This is supported by the literature. For instance, GLA states that they are worried about the over-reliance on GPS. This is strong evidence that GPS is indeed crucial, since an over-reliance is also self-reinforcing. The more you rely on it, the more crucial the system gets. Several also state in their comments that the lack of personnel to staff other means plays a role in this. This is supported by literature.

If we move to figure 11 of the results section, we see that 40% consider it to be manageable for someone to transmit false GPS signals to a vessel. A little over 23% consider it to be easy, while 20% say it is difficult. If we compare this to the literature overall, manageable is a fair assessment of the situation. We will not site the comments made here, but they can be seen in full in the results section. All comments reflect that the respondents think it would be easy to jam and difficult to spoof. The literature support that it would be easy to jam the GPS signal. Lysne states that it would be easy for a passenger to jam the GPS signals by bringing low-tech and low-cost jamming equipment with him on board. They also talk about small jammers mounted on drones. GLA takes it one step further, and actually successfully jam a geographical area at sea. On the other hand, the literature does not support that GPS is difficult to spoof. Shepard and Humphreys states that GPS is inherently susceptible to spoofing. They say that an attacker can easily detect how the legitimate GPS signals are detected by the receiver. This will enable the attacker to design a similar signal, but with their own geographical data. The lack of sender authentication in the civilian GPS system enables the attacker to transmit the modified signal to the vessel. The University of Texas, under the lead of Humphreys, has also performed real-life experiments to uncover how easy GPS spoofing would be. In August 2017, the Norwegian industry newspaper Digi.no, reported about actual incidents of GPS spoofing in the Black Sea.

If we now move to figure 13 of the results section, we can see that 50% of the respondents say that spoofing of the GPS service would result in a small reduction in the crew's ability to avoid accidents at sea. This cannot be said to be in line with the literature, and also indicate some flawed internal logic. It is interesting that the respondents generally consider GPS to be important or very important to avoid accidents, but that the manipulation of it would only cause a small reduction in ability. This indicate some lack of awareness, since the respondents are clearly not able to make the connection between the two. The comments include a lot of ifs and buts on this question. Most of them revolve around the question if the spoofing is detected or not, and if the crew is using other means of navigation for redundancy. One comments sums it all up nicely, and is also supported in the literature: "Crews are not accustomed to navigating without GPS.". GLA comment that it would be problematic for the crew to revert back to old fashion methods, due to lack of staff and experience. Provided that they are able to detect the issue at hand. GLA also state that if the issue is not detected, it would impact the sailing safety gravely. The literature also provides us with several scenarios where loss or modification of the GPS signal could be severely problematic. Lysne comment that loss of trustworthy satellite navigation while "hovering" in close proximity to an oil installation, could result in a critical failure of the DPS. GLA also uncovered in their field experiments that the loss of GPS would kill both the AIS and the ECDIS on board.

In question 11 we asked the respondents to comments if they knew of any countermeasures that can be used to mitigate attacks using false GPS signals. Other means of navigation is mentioned several times, both eLoran, visual, inertial and celestial navigation is mentioned. The same trend is seen in the literature. ELoran is mentioned by several sources. One especially interesting comment highlights the issue of awareness: "Having someone with IT experience onboard, and also working with coastguard, VTS services and also working with other vessels in the area to conduct periodical GPS signal and position confirmations". This might indicate that there are concerns about not having tech-savvy and aware staff on board. This is supported by literature.

5.2 AIS

The first question related to AIS is found in question 6 of the electronic questionnaire. Here we can see that half of the respondents find it to be somewhat important in preventing accidents at sea. This trend can be observed further in some of the comments. One say: “AIS is an information service NOT a collision avoidance device”. Another say: “AIS is not reliable, will be secondary sensor after radar or visual”. The important of the actual OOW (Officer of Watch) is stated one of many times: “Helps to positively identify targets. However it is defenitly the cause of accidents when poor OOW’s use it for collision avoidence”. In addition, this comment once again point out that the crew might not view AIS as a collision avoidance aid. Nevertheless; one third of the respondents also consider it to be important. Some of the comments also reflect this view. The literature does not support the claim that AIS is not a collision avoidance tool. Trend Micro also states this. In addition, Trend Micro says that AIS is one of the most important wireless technologies used at sea, and that it is a crucial tool in traffic monitoring and vessel assistance.

In question 8, we see that 26.67% view it as very easy to transmit false AIS signals to a vessel, while half of the respondents find it easy. This reflects the literature. Trend Micro compiled a large list of activities they were able to perform in the AIS system, with limited means. Lysne also list the lack of protection against signal modification in AIS amongst their top 10 digital vulnerabilities in the maritime sector. The comments made on this question is rather ambivalent, and doesn’t really pull in any specific direction. There were also only 4 comments made; possible due to the polarized view on this matter. AIS is viewed as insecure by the respondents; with good cause.

In question 10 we observe an interesting pattern. When asked to rate how false AIS signals would affect the ability to prevent accidents, 20% say that it will cause a substantial reduction in ability, 40% small reduction, and another 40% no reduction. This correlates nicely with the answers on question 6, where the respondents were quite unison in their view on the importance of AIS in collision avoidance. It is not surprising that we see the respondents place themselves with 80% on no reduction or small reduction, when the general view is that AIS is overall not that important.

6 Conclusion

After reviewing the initial problem description and hypothesis, the literature and the results from the survey, we can reach a conclusion on both research questions. On research question 1, we can conclude that the maritime stakeholders are somewhat aware of the security issues in the wireless technologies they utilize. The respondents are aware that there are indeed security issues, but does not contemplate the full scale of it. On research question 2, we can conclude that maritime stakeholders does consider the potential lack of information security as a smaller security concern than the literature. This is especially true for AIS. If we look at both research questions as a whole, the respondents are showing wears of being a little optimistic about both system security and potential impact. That said, we do not see any signs of non-existing information security awareness in this particular survey.

We see that the sector views GPS as important to security, which is supported by literature. The comments indicate that the importance is linked to lack of staff, and lack of ability to revert to other means of navigation. When assessing how difficult it would be to transmit false GPS signals to the vessel, the majority place themselves from manageable to very easy. This is also supported by literature. The comments on the other hand, indicates that the respondents view jamming as the easy task, and that spoofing of the system would be quite difficult. This is not supported by literature. We also see a break of logic when the respondents are asked how received false GPS signals would affect their ability to prevent accidents at sea. Here we see that 50% assess it to have a small impact. This is not supported by literature. It also seems odd to claim that GPS is very important to prevent accidents, partly due to lack of staff and other skills, and then assess that a loss of the system would cause a small reduction in ability to prevent accidents.

Regarding AIS, the survey revealed some surprising findings as well. We saw that 80% of the respondents rated that receiving false AIS signals would have a small or no reduction in the vessel's ability to avoid accidents at sea. This links up with the initial hypothesis. But in connection with this, we also observed that 50% of the respondents rated that AIS was somewhat important in preventing accidents at sea. This was further reflected in the comments. Therefore, we cannot say with certainty if the security impact is downplayed due to low awareness, or due to the fact that the respondents really do not find AIS that important in accident prevention. The comments do not clarify in satisfying detail why AIS is not considered to be a collision avoidance system by the respondents. When it comes to the degree of difficulty of transmitting false AIS signals to the vessel, the majority range from easy to very easy. This is in line with the literature.

If we look at all this, we cannot fully claim that the information security awareness is low. But we do see a trend where the importance of AIS, and the impact of compromised GPS, is downplayed. The reasons are not clear to us. It can of course be linked to low awareness, or a flawed conceptual overview. But it can also be linked to parameters we have not considered or even anticipated.

Note that the conclusions made in this thesis are not measured against the level of awareness in other sectors, and that we have only looked at two specific maritime communication systems; namely GPS and AIS. It is also important to note that the number of respondents is not sufficient to apply the results to the whole chosen population, but enough to be able to observe trends and indications.

6.1 Future work

With only 30 completed responses in the survey, the results can only be applied to look for trends. To investigate this phenomena in detail, future work could include a larger survey performed by professionals. I.e. a survey with enough respondents to make the results statistically significant. By doing that, we can look at the perceptions of the sector in detail by applying statistical methods.

Also, some of the findings in this thesis are interesting and somewhat confusing at the same time. It would be interesting to do a similar project as a case study of a specific vessel, company or similar. Then we could go into more detail on the areas where it gets interesting, or on areas that need some clarification.

Bibliography

[1] Lysneutvalget. Digitale sårbarheter maritim sektor. Technical report, DNV GL, 2015.

[2] Cimpean, D., Meire, J., Bouckaert, V., Casteele, S. V., & A. Pell and, L. H. Analysis of cyber security aspects in the maritime sector. Technical report, ENISA, 2011.

[3] Grant, A., Williams, P., Ward, N., & Basker, A. 2009. Gps jamming and the impact on maritime navigation. *Journal of Navigation*, 62(2), 173–187.

[4] Shepard, D. & Humphreys, T. 2012. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3), 146–153.

[5] News, U. 2013. Ut austin researchers successfully spoof an $80 million yacht at sea. https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea. Accessed: 2017-06-15.

[6] Digi.no. 2017. Falske gps-signaler narret navigasjonsutstyret til flere titalls skip. https://www.digi.no/artikler/falske-gps-signaler-narret-navigasjonsutstyret-til-flere-titalls-skip/399100. Accessed: 2017-12-07.

[7] Balduzzi, M., Pasta, A., & Wilhoit, K. 2014. A security evaluation of ais automated identification system. 436–445, New York, NY, USA. ACM.

[8] Strohmeier, S., Schäfer, M., Pinheiro, R., Lenders, V., & Martinovic, I. N/A. On perception and reality in wireless air traffic communication security. *N/A*, N/A(N/A), N/A.

[9] Oates, B. 2006. *Researching Information Systems and Computing*. Sage.

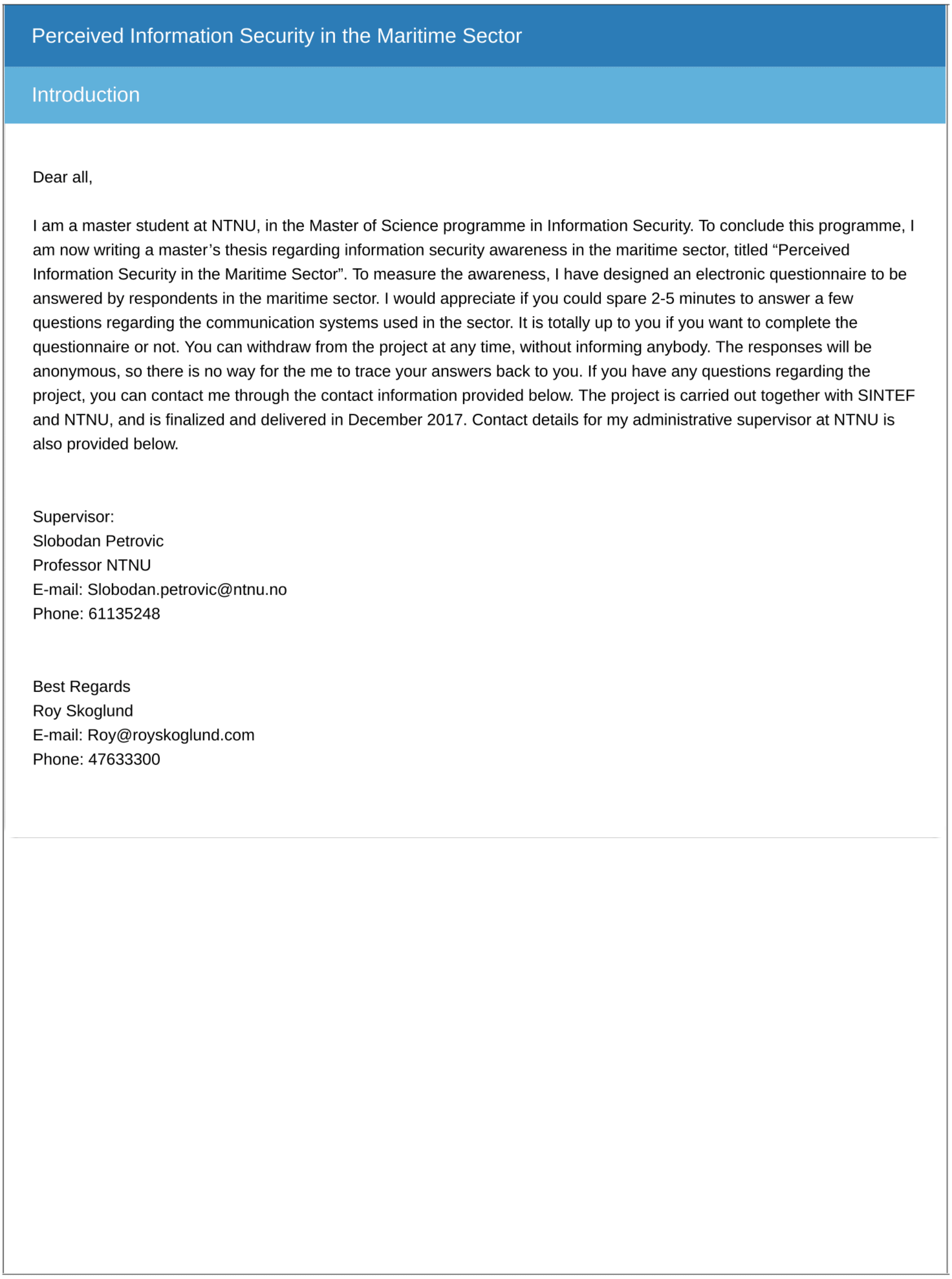
[10] Regjeringen.no. 2017. Maritime næringer. https://www.regjeringen.no/no/tema/naringsliv/maritime-naringer/id1337/. Accessed: 2017-03-17.

[11] SurveyMonkey.com. 2017. Calculating the number of respondents you need. https://help.surveymonkey.com/articles/en_US/kb/How-many-respondents-do-I-need. Accessed: 2017-12-14.

[12] SurveyMonkey.com. 2017. Sample size calculator. https://www.surveymonkey.com/mp/sample-size-calculator/?ut_source=help_center. Accessed: 2017-12-14.

A Appendix

A.1 Electronic questionnaire with associated information letter



Perceived Information Security in the Maritime Sector

Introduction

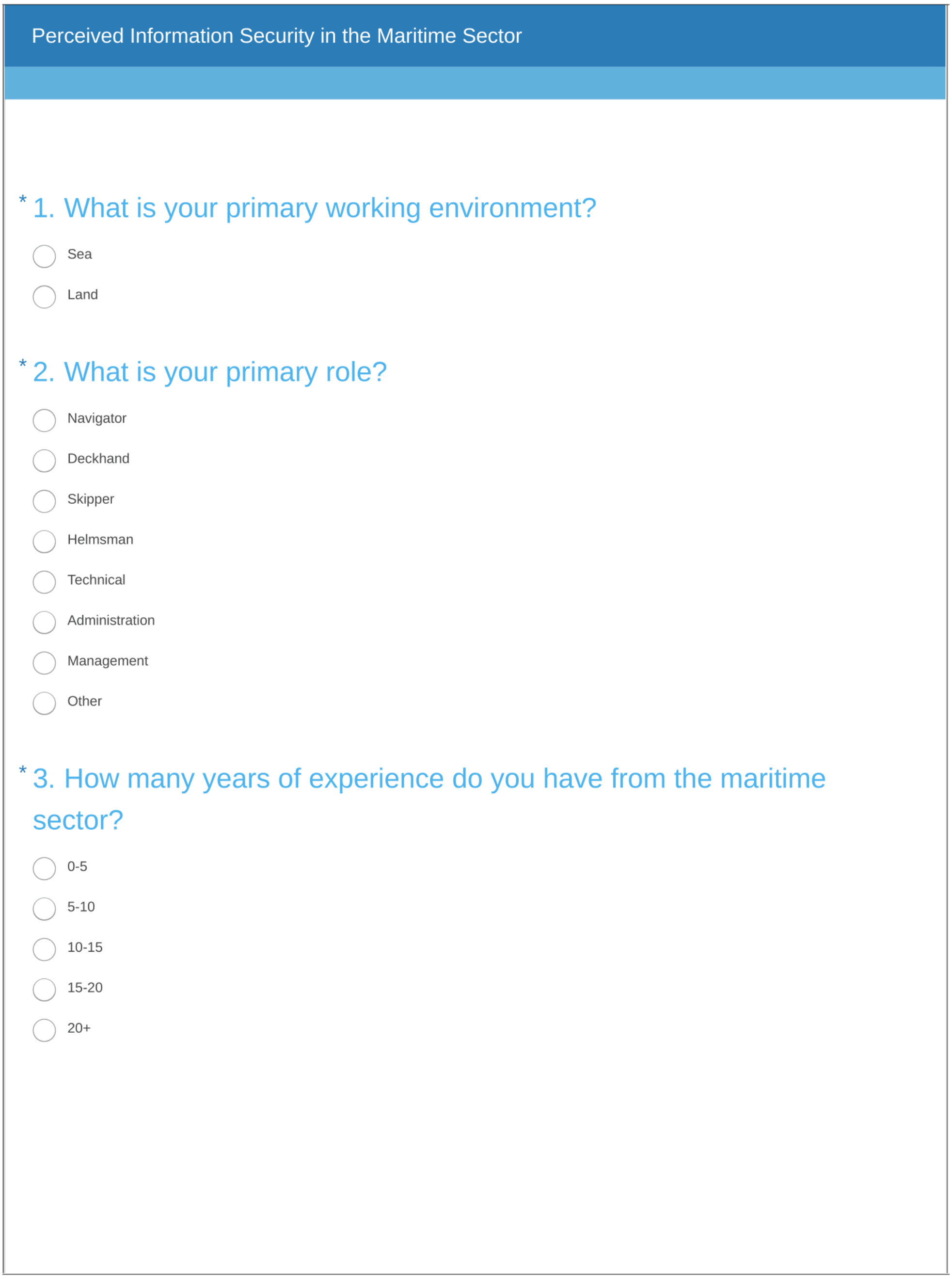
Dear all,

I am a master student at NTNU, in the Master of Science programme in Information Security. To conclude this programme, I am now writing a master's thesis regarding information security awareness in the maritime sector, titled "Perceived Information Security in the Maritime Sector". To measure the awareness, I have designed an electronic questionnaire to be answered by respondents in the maritime sector. I would appreciate if you could spare 2-5 minutes to answer a few questions regarding the communication systems used in the sector. It is totally up to you if you want to complete the questionnaire or not. You can withdraw from the project at any time, without informing anybody. The responses will be anonymous, so there is no way for the me to trace your answers back to you. If you have any questions regarding the project, you can contact me through the contact information provided below. The project is carried out together with SINTEF and NTNU, and is finalized and delivered in December 2017. Contact details for my administrative supervisor at NTNU is also provided below.

Supervisor:
Slobodan Petrovic
Professor NTNU
E-mail: Slobodan.petrovic@ntnu.no
Phone: 61135248

Best Regards
Roy Skoglund
E-mail: Roy@royskoglund.com
Phone: 47633300

Figure 15: Page 1 of the questionnaire.



Perceived Information Security in the Maritime Sector

* 1. What is your primary working environment?

○ Sea

○ Land

* 2. What is your primary role?

○ Navigator

○ Deckhand

○ Skipper

○ Helmsman

○ Technical

○ Administration

○ Management

○ Other

* 3. How many years of experience do you have from the maritime sector?

○ 0-5

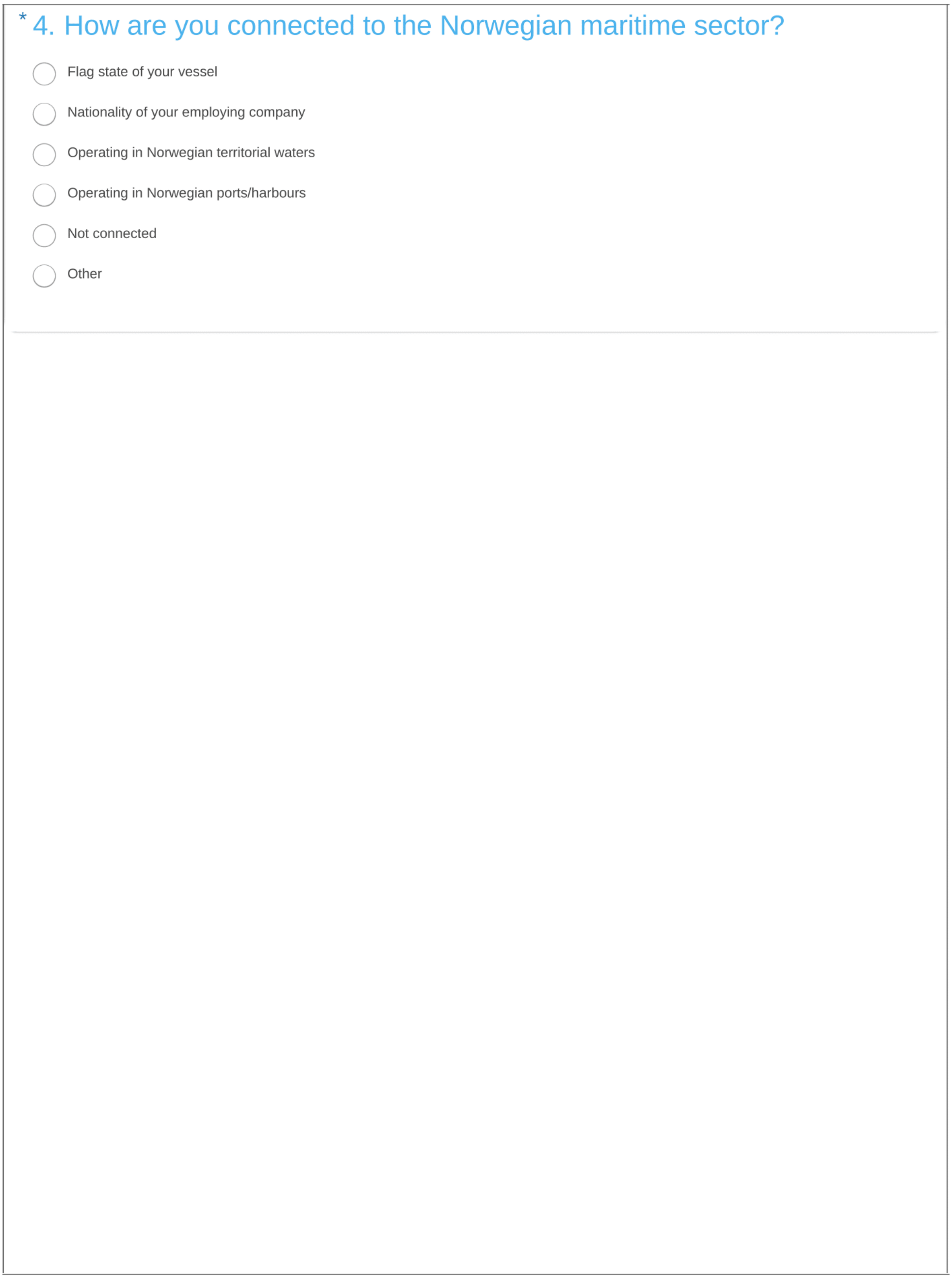
○ 5-10

○ 10-15

○ 15-20

○ 20+

Figure 16: Page 2 of the questionnaire.



* 4. How are you connected to the Norwegian maritime sector?

○ Flag state of your vessel

○ Nationality of your employing company

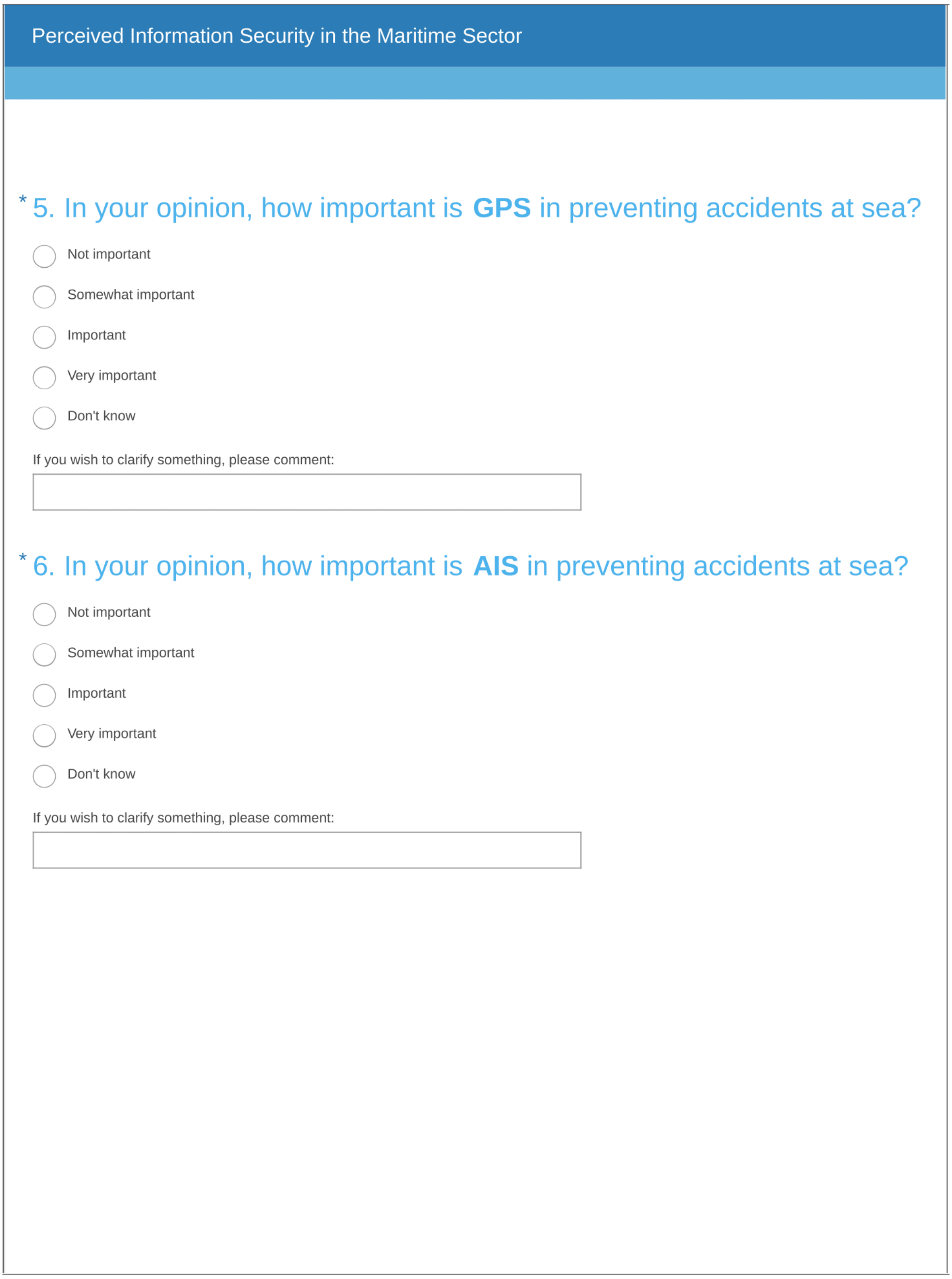
○ Operating in Norwegian territorial waters

○ Operating in Norwegian ports/harbours

○ Not connected

○ Other

Figure 17: Page 3 of the questionnaire.



Perceived Information Security in the Maritime Sector

* 5. In your opinion, how important is **GPS** in preventing accidents at sea?

○ Not important

○ Somewhat important

○ Important

○ Very important

○ Don't know

If you wish to clarify something, please comment:

* 6. In your opinion, how important is **AIS** in preventing accidents at sea?

○ Not important

○ Somewhat important

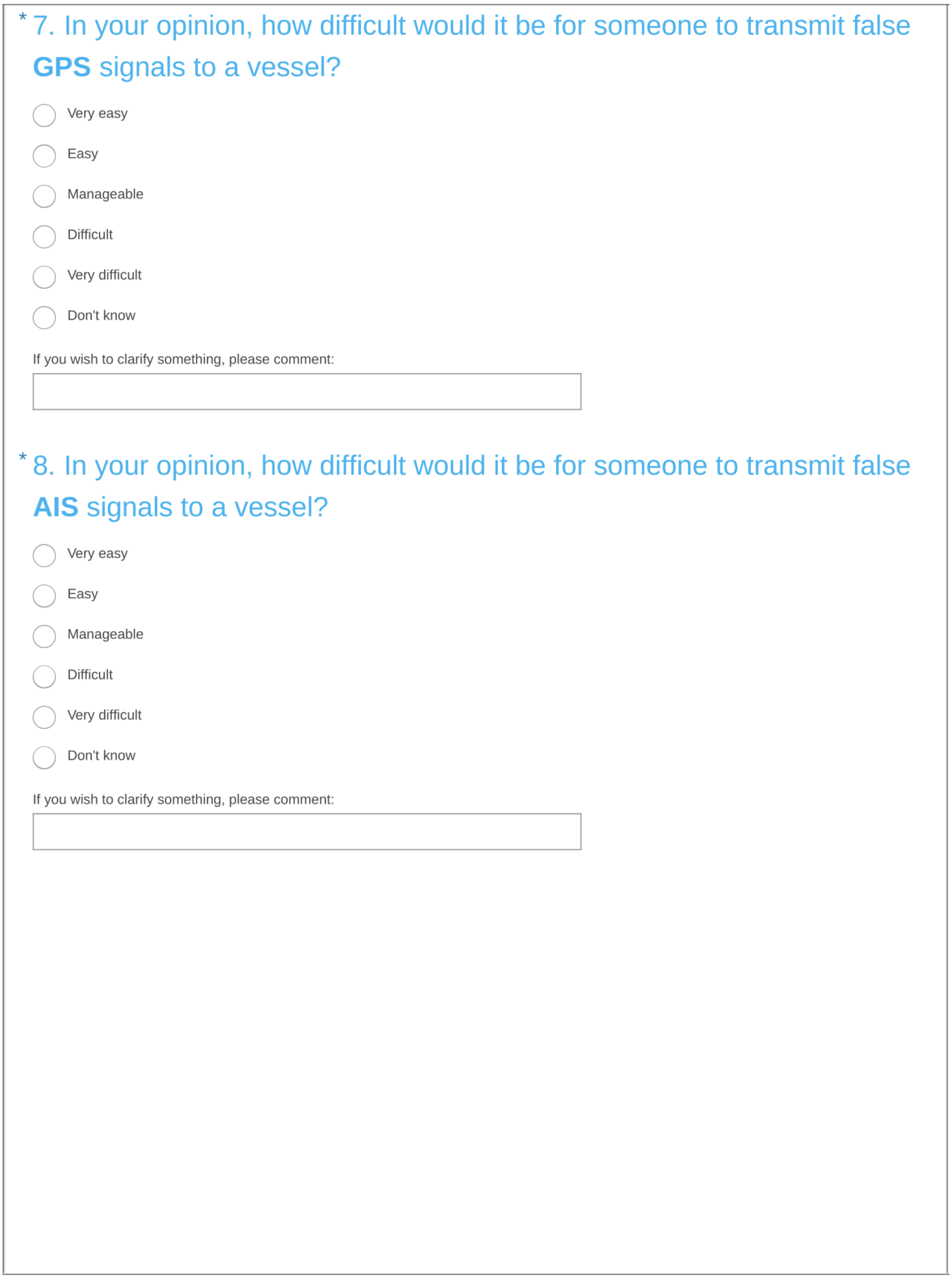
○ Important

○ Very important

○ Don't know

If you wish to clarify something, please comment:

Figure 18: Page 4 of the questionnaire.



* 7. In your opinion, how difficult would it be for someone to transmit false **GPS** signals to a vessel?

○ Very easy

○ Easy

○ Manageable

○ Difficult

○ Very difficult

○ Don't know

If you wish to clarify something, please comment:

* 8. In your opinion, how difficult would it be for someone to transmit false **AIS** signals to a vessel?

○ Very easy

○ Easy

○ Manageable

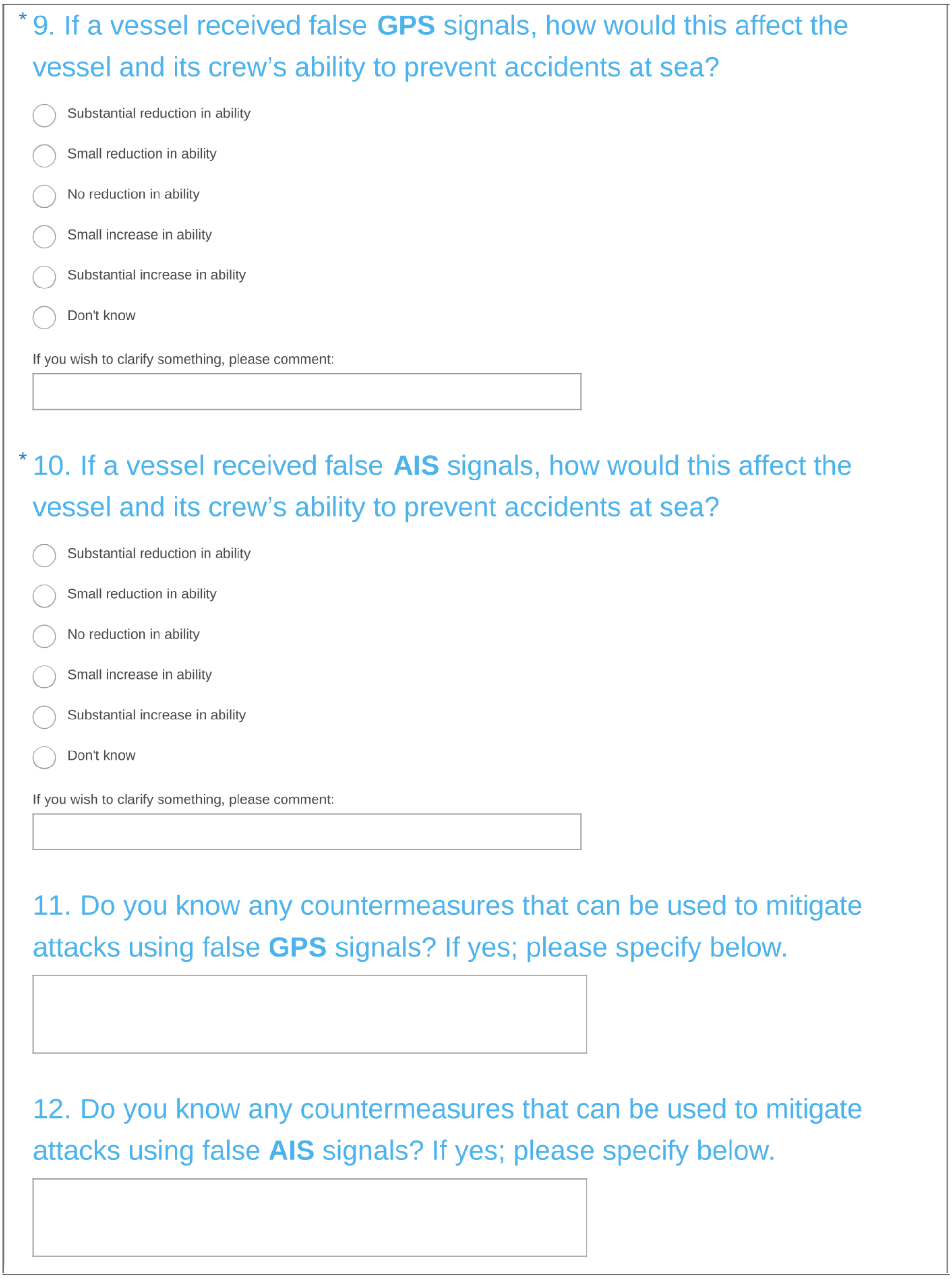
○ Difficult

○ Very difficult

○ Don't know

If you wish to clarify something, please comment:

Figure 19: Page 5 of the questionnaire.



* 9. If a vessel received false **GPS** signals, how would this affect the vessel and its crew's ability to prevent accidents at sea?

○ Substantial reduction in ability

○ Small reduction in ability

○ No reduction in ability

○ Small increase in ability

○ Substantial increase in ability

○ Don't know

If you wish to clarify something, please comment:

* 10. If a vessel received false **AIS** signals, how would this affect the vessel and its crew's ability to prevent accidents at sea?

○ Substantial reduction in ability

○ Small reduction in ability

○ No reduction in ability

○ Small increase in ability

○ Substantial increase in ability

○ Don't know

If you wish to clarify something, please comment:

11. Do you know any countermeasures that can be used to mitigate attacks using false **GPS** signals? If yes; please specify below.

12. Do you know any countermeasures that can be used to mitigate attacks using false **AIS** signals? If yes; please specify below.

Figure 20: Page 6 of the questionnaire.