Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Risk from cyberattacks on autonomous ships

Jan Erik Vinnem & Ingrid Bouwer Utne
Department of Marine Technology, NTNU, Norway

ABSTRACT: The vulnerability of technological and administrative systems to cyberattacks has been shown to be high in several cases, which has led to different unwanted consequences. Autonomous ships will also be exposed to the threat of cyberattacks, due to their need for connecting to operational, management and administrative systems onshore. The most critical hazards are possibly not associated with consequences for the ship itself or its cargo, but the threat to infrastructure along the coast and offshore if a ship under alien command is used as a "battering ram" to cause major structural damage. Even relatively small autonomous ships may pose a real threat, and ships sailing in international waters may come from distant locations. This implies that all autonomous ships may be considered as possible threats. This paper outlines the risk for some infrastructure systems. Even though the probability may be low, such events cannot be ruled out in the future, and the design of autonomous ships must involve a series of risk reducing actions and designs.

1 INTRODUCTION

Maritime security has come on the agenda the past decade. In 2004, the U.S. presented a national maritime security policy. The Sept. 11th attacks also put maritime terrorism on the agenda. The increase in piracy attacks in 2008 and 2011 outside the coast of Somalia contributed to even more attention to maritime security globally. In 2011, maritime security became one of the objectives in The North Atlantic Treaty Organization's (NATO) Alliance Maritime Strategy. The UK, EU and the African Union proposed maritime security strategies in 2014 (Bueger, 2015). The Maritime Safety Committee (MSC) in the International Maritime Organization has recently published guidelines on maritime cyber risk management (IMO, 2017a).

There is an increased focus on developing autonomous ships. A motivation is reduced building and operational costs, because the ships can be redesigned. Research projects, such as the Maritime Unmanned Navigation Through Intelligence in Networks (MUNIN) (Rødseth & Tjora, 2014) and Advanced Autonomous Waterborne Applications (AAWA, 2016) focus on the development of technological specifications and designs for autonomous ships. Industry projects aim at realizing the first autonomous ships in the next 1–3 years, e.g., Yara Birkeland (Kongsberg Maritime, 2017).

Autonomous ships will be exposed to the threat of cyberattacks, due to their need to connect to operational, management and administrative systems onshore. The most critical hazards are possibly not associated with consequences for the ship itself or its cargo, but the threat to infrastructure along the coast and offshore if a ship under alien command is used as a 'battering ram' to cause major structural damage. Even relatively small autonomous ships represent a high kinetic energy when travelling at full speed and may thus pose a real threat to infrastructure systems. Ships sailing in international waters may come from distant locations. This implies that all autonomous ships may be considered as possible threats. It will not be sufficient to ensure that the high-quality classification societies have stringent requirements; all classification societies or IMO need to focus on such threats.

We may think that the probability of cyberattacks may be low, but such events cannot be ruled out in the future. We therefore believe that it is important, before autonomous ships are built and commissioned, that the marine and maritime industry at large, consider this threat and takes necessary actions to implement sufficient risk control actions.

A cyber-attack may have some parallels with the terrorist attack on USS Cole, the United States Navy guided-missile destroyer, on 12th October 2000, while it was being refueled in Yemen's Aden harbor (US Navy, 2001). 17 sailors were killed and 39 injured, due to the attack from a small fiberglass boat carrying explosives and two suicide bombers. The boat approached the port side of the destroyer in bright daylight, and exploded, creating a 12 by 18 m gash in the ship's port side from what was estimated to 180–320 kg of explosives.

The objective of the paper is to discuss the implications of the vulnerability of autonomous ships to cyber-attacks, the threats that a ship under alien control may represent for infrastructure systems, and how such risk should be mitigated in general. There are also other activities and sectors in the society where cyber-attacks may be a potential threat. One incident known from the petroleum industry is described in Section 2.1. Some incidents in the energy sector are briefly mentioned in Section 2.3. Autonomous cars are another such sector, see further descriptions in Section 2.2. Experiences from other sectors can be used as a basis for assessing risk and developing relevant risk mitigation measures for autonomous ships.

Traditional risks to ships, which also apply to autonomous ships, such as collision, grounding, foundering, etc. are outside the scope of the paper, and are therefore not discussed. These risks are still important, and are subject to attention by several researchers. The risks to infrastructure systems are special in the sense that catastrophic consequences may cascade outside the industry itself.

The paper considers unmanned autonomous ships primarily, but differences between unmanned and manned autonomous ships are also considered.

2 REVIEW OF CYBER THREATS IN COMPARABLE SYSTEMS

2.1 *Petroleum industry*

It is not easy to collect experience data about cyber-attacks. Statoil corporate management was invited to give a university lecture about cyber threats to their systems and operations in October 2016 (Statoil, 2016). The incidents presented during this lecture are presented in Section 2.3 below. No incidents were mentioned in the lecture from Statoil's own operations. Three weeks later it was revealed through media that there had been a serious unintended incident at Statoil's Mongstad refinery in May 2014, as described in the following. Through the subsequent handling of this incident, it became clear that Statoil has had many more incidents of probably different severity. What was revealed by media a short while after the guest lecture puts the lack of openness in the university lecture in a special light.

The most well-known incident in the petroleum industry is from the downstream part, where maintenance on a server by an IT specialist in Hindustan Computers Ltd. (HCL) in India disrupted the loading of a gasoline tanker at the Statoil operated Mongstad refinery just outside Bergen in Norway on 21st May 2014. An input error by the operator gave him access to a server he should not be able to access. It should not be possible to stop the server in question remotely, but the HCL specialist inadvertently accessed the server through a 'back door', according to media.

The operations of certain IT systems, including the Mongstad refinery, was outsourced by Statoil to HCL in India in 2012, after a risk assessment. The incident referred to here did not affect safety directly, but could potentially have affected safety functions and barriers, according to the audit report by Petroleum Safety Authority (PSA, 2017).

The NRK broadcasting company in Norway found 29 incidents where information and communication technology (ICT) employees from India had accessed servers they should not have access to in Statoil. Anonymous sources in Statoil have commented that the problem was more extensive than what the journalists found.[1]

The PSA audit was initiated after the incident was known in the public domain, almost 2.5 years after it occurred. The audit considered the handling of incidents associated with ICT and information security by Statoil in general. PSA considered several ICT related incidents, as well as Statoil's technical requirements to information security for industrial automation and control systems. The wording of the PSA audit report is such that it indicates that other incidents have occurred that are unavailable in the public domain.

Statoil was criticized by PSA for failing to notify the authorities about the incident at the time it occurred, which according to Statoil's own assessment could have had consequences, such as failure of safety functions or barriers, according to media reports (see footnote[1] above).

Statoil informed in mid 2017 that they had cancelled all outsourcing contracts that affected safety critical systems. They had concluded that the outsourcing of these systems represented too high risk for unwanted influence on the systems.

From the media, it is known that Statoil was the target of a massive attack over three days in 2013, where hackers tried to install dangerous code into Statoil computers[2], apparently an unsuccessful attack.

2.2 *Autonomous vehicles*

Autonomous cars are expected to become an important part of the transportation system within the next decade. Self-driving vehicles will

[1]https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013.
[2]http://www.newsinenglish.no/2014/08/28/statoil-held-off-hacker-attack/.

be shared by several users (Lyche, 2017). Autonomous buses may be realized in the near future with operators in control centers remotely overseeing several buses. In specific circumstances, the operators may take over control and remotely operate the buses if needed (Lyche, 2017). This means that the autonomous buses will operate in different autonomy levels, with shared control.

A major challenge is the increasing interconnection that may expose safety-critical systems to security threats. Cars are no longer physically isolated machines controlled mechanically and locally (Macher et al, 2017). They have become computers with various electronic control units (ECU) and hackers may take control over brakes, engine, the steering wheel, radio, and lights. Recently, it was discovered that one million cars could be hacked simultaneously (Kibar, 2017; Slovik, 2017).

A car's vulnerability to hacking depends on what kind of remotely connection the car has, the configuration of the car's internal computer network, and how external digital commands may affect physical components (Kibar, 2017). Press (2017) discusses how cars can become weapons of mass destruction on the road. It will not be sufficient to install firewalls or intrusion detection systems. The UK Government states that Wi-Fi connected cars along with autonomous cars are getting increasingly vulnerable to hacking and data theft. They recently published key principles of vehicle cyber security for connected and automated vehicles to support the industry (GOV.UK, 2017). These principles are (quote):

1. Organizational security is owned, governed and promoted at board level.
2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.
3. Organizations need product aftercare and incident response to ensure systems are secure over their lifetime.
4. All organizations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.
5. Systems are designed using a defence-in-depth approach.
6. The security of all software is managed throughout its lifetime.
7. The storage and transmission of data is secure and can be controlled.
8. The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

The connectivity means that the vehicle is integrated in a global ad-hoc network system where external information are important for decision making. Security has become an important aspect to include in systems safety engineering. The development of these novel transportation systems means that systematic approaches taking both safety and security aspects into consideration are needed (Macher et al, 2017).

Standards relevant for the automotive domain are increasing their focus on security. IEC 61508:2010 mentions that security threats may be identified during hazard analysis. Nevertheless, the security threat analysis is not specified or detailed. The SAE J3061:2016 is a guideline for cybersecurity engineering. Among other things, it focuses on defining a process for implementing cybersecurity in the design, considering a vehicle's lifecycle and providing basic guiding principles on cybersecurity.

2.3 *Energy sector*

Some other cyber-attacks on the energy sector that are known in the public domain are the following (Statoil, 2016):

- Attacks on Technical network
  - Stuxnet: Iran's uranium enrichment facility 2010
  - German Steel Mill 2014
  - Ukrainian power network 2015
  - German nuclear plant 2016
- Attacks on Office network
  - Shamoon incident: Saudi Aramco office network 2012
  - Energetic Bear: Energy industry in the US and Europe 2012 →
  - Cleaver (recon): Energy infrastructure several countries around the globe 2012 →

The Gundremmingen nuclear power plant in Germany, located about 120 km northwest of Munich, is run by the German utility company RWE. It was found to be infected with computer viruses, but they appeared not to have posed a threat to the facility's operations because it is isolated from the Internet, according to press reports.[3] The viruses, which included "W32.Ramnit" and "Conficker", were discovered at Gundremmingen's B unit in a computer system retrofitted in 2008 with data visualisation software associated with equipment for moving nuclear fuel rods, RWE said. Malware was also found on 18 removable data drives, mainly USB sticks, in office computers maintained separately from the plant's operating systems. W32.Ramnit is designed to steal files from infected computers and targets Microsoft

[3] http://www.telegraph.co.uk/news/2016/04/27/cyber-attackers-hack-german-nuclear-plant/.

Windows software, according to the security firm Symantec. Conficker has infected millions of Windows computers worldwide since it first came to light in 2008. It is able to spread through networks and by copying itself onto removable data drives, Symantec said.

The 'Energetic Bear' is a Russian virus that let hackers take control of power plants. Over 1,000 energy firms have been infected, according to media reports.[4]The hackers obtained access to power plant control systems, and could have disrupted energy supplies in affected countries, if they had used the sabotage capabilities open to them, according to Daily Mail.

In October 2017, it has been revealed by media[5] that Russians have jammed the GPS signals in Northern Norway in September 2017, as a deliberate action by Russian militaries during a cyber warfare exercise.

3 CYBER RISKS FOR AUTONOMOUS SHIPS

3.1 *Hacking of autonomous ships*

The technological advancements towards ships operating without an onboard crew is enabled by the developments in ICT in recent years. ICT provides data connection and on-board intelligence and data connection capabilities. The ships may operate in different levels of autonomy. In a high level of autonomy, ships may be supervised by human operators in Shore Control Centres (SCC). Whenever necessary, the operator (supervisor) may intervene. A SSC could take responsibility for overseeing specific phases of a ship's operation or voyage, for example, maneuvering in and out of port, which then means that the ship would operate in a lower level of autonomy. The connectivity between the ship and SSC must have high capacity and availability and is crucial for the realization of autonomous ships (AAWA, 2016; MUNIN, 2015).

The increasing usage of networked ICT technology makes it possible to access systems through net-work interfaces and gain unauthorized remote capability to control ship systems in undesired manners (AAWA, 2016). Security threats that are relevant for ships are piracy and highjacking, smuggling of goods, human trafficking, damaging of ship or port facility, vandalism, sabotage, such as intentional jamming or spoofing of the ship automatic identification system (AIS), GPS signals and communication systems, and use of the ship as weapon for terrorist activity (AAWA, 2016; MUNIN, 2015).

The security challenge of shipping has been addressed by the International Maritime Organization (IMO) Maritime Safety Committee and The Facilitation Committee, who recently issued guidelines on maritime cyber risk management (IMO, 2017a). The guidelines give high-level recommendations on security risk management to protect shipping from current and emerging threats. Five functional elements are presented consisting of identification, protection, detection, responding and recovering. Vulnerable systems that are mentioned in the guideline are bridge systems, cargo handling and management systems, machinery and propulsion systems, control systems, passenger servicing and management systems, passenger public networks, crew welfare systems, and communication systems. IMO states that cyber risk management should be integrated into ship safety management within 2021 (IMO, 2017b).

To protect a ship against cyber threats means that vulnerabilities in the ICT infrastructure need to be eliminated and effective measures for intrusion prevention must be implemented. It is also necessary to consider that hackers may become more skillful over time with more advanced techniques available. This means that cyber security needs to be dynamic and proactive. Classification and encryption of data, user identification, authentication, authorization, protection of data integrity and connectivity, as well as activity logging and auditing are examples of typical cyber security methods that are expected to be needed (AAWA, 2016).

MUNIN (2015) presents a risk matrix, including both safety and security aspects. The highest ranked threats are found to be jamming, spoofing or hacker attacks of AIS, GPS signals, or communication systems, leading to collision with other ships, or ship grounding in critical areas.

3.2 *Autonomous ships used as threat to infrastructure systems*

The control over an unmanned ship which is hacked may be lost completely, which is the most severe situation. It is assumed that complete loss of control is impossible if there is a small crew onboard. It is assumed that a small crew may be able to deactivate external control and take over control locally. If this fails, they should at least be able to shut of power and let the ship drift until they may be able to take back control locally.

But without local crew such possibilities are not available, and control may be lost completely, at least for some time. In theory, control may be

[4]http://www.dailymail.co.uk/sciencetech/article-2675798/Hundreds-European-US-energy-firms-hit-Russian-Energetic-Bear-virus-let-hackers-control-power-plants.html.

[5]https://www.nrk.no/finnmark/e-tjenesten-bekrefter_-russerne-jammet-gps-signaler-bevisst-1.13721504.

reestablished by boarding the ship, for instance by helicopter, such as police helicopter or naval helicopter. This will take time in any case, and if the vessel is far from shore, a helicopter may not be able to reach the ship until it comes closer to shore, and then it may be too late.

It is therefore possible that an unmanned, autonomous ship that has been hacked may be used to ram into infrastructure systems. This is discussed further below. A similar scenario could also occur with a conventional manned ship, if the ship is highjacked, but this is outside the scope of the present discussion.

Let us first consider if a hacked, unmanned ship may be a threat to other ships in open seas. This may be possible in principle, but if the other ships are conventional, manned ships, they may be able to avoid the hacked, unmanned ship through maneuvering away from the threat. This may fail if the threat is not observed, but should normally be successful. It the second ship is an unmanned, autonomous ship, control from shore should be able to observe the threat in a similar manner.

A special case occurs if other ships represent potential extreme catastrophic consequences, for instance if the other ship is a cruise ship with many thousands of cruise passengers. Or if the other ship is a very (or ultra) large crude carrier, capable of transporting in order of 2,000,000 bbls of crude oil. These ships would not be autonomous, and should normally be able to avoid attack.

But infrastructure installations are usually stationary and not able to relocate to avoid the threat. By infrastructure systems in this context one may first of all think of bridges crossing fjords and bays and other seawater open areas which are found in almost all coastal areas worldwide. Other systems may be offshore petroleum installations, which are found far away from shore in several parts of the world; the North Sea, Gulf of Mexico, Atlantic Sea off the coast of Brazil, several African countries, Newfoundland, Shetland as well as the Pacific in some areas off Australia and the South China Sea.

There are considerable differences with respect to impact resistance to external impact in the various types of infrastructure systems. In Norway for example, there has been a study project ongoing to establish possible concepts for fjord crossing of some of the largest fjords on the West coast of Southern Norway. For a possible fjord crossing of the Sognefjord, a floating bridge concept has been specified to have 1563 MJ kinetic energy resistance, corresponding to a ship of about 31,500 tdw, travelling at a full speed of 17.7 knots (Statens Vegvesen, 2013). Smaller bridges along the coast are believed to have resistance at least one order of magnitude lower, but the consequences of a collision against a smaller bridge may be less extensive.

When it comes to offshore structures, the traditional resistance has been designed to take the impact from a drifting service vessel. Typically, this was a value of 14 MJ for many years (Vinnem, 2013), but is in recent years increased to around 50 MJ (Yu & Amdahl, 2018), due to increasing size of service vessels used for these installations. The largest offshore structures, the concrete gravity based structures (so-called Condeep structures), which we commonly installed in the North Sea some 20 years ago, have a push-over resistance about 200 MJ (Vinnem, 2013). This is almost an order of magnitude lower than the specified resistance of the bridge for the fjord crossing of the Sognefjord. Most of the offshore structures have capacity in the order of 50 MJ or less.

Floating offshore structures may in theory move away, if threat is detected sufficiently early. If the hacked ship is used with the intention to ram into a structure, it may be able to follow the movements of the offshore installation.

Even a small ship with a mass of 5,000 tons, travelling at a speed of 12 knots, has a kinetic energy of roughly around 200 MJ, which is excessive in relation to structural capabilities of most offshore structures; only the Condeep structures could be expected to survive. Larger ships will be a threat to all offshore structures.

The largest offshore structures are usually manned with up to a few hundred persons, implying that many lives are at risk. In addition, comes the blowout potential. Here the fixed installations are the most vulnerable, because the equipment to isolate the wells are mainly on deck. If the installation is wiped out, very long-lasting blowouts may occur as a result, in addition to the death toll.

4 FEASIBILITY OF RISK REDUCTION

4.1 *Approach to risk control*

The previous sections have shown that hacked autonomous unmanned ships may be a considerable threat to offshore installations, and to infrastructure elements along the coast unless particularly strengthened.

It is considered that further strengthening of constructions is not relevant. First of all, this is impossible for existing structures, and further strengthening of future structures is not relevant due to excessive costs. The risk control actions will need to be focused on prevention of the threats to cause incidents.

Traffic surveillance is one of the solutions adopted by the offshore oil and gas industry for protection of offshore installations against collision threats by passing vessels. For the Norwegian sector, there are several centers; two operated by off-

shore companies and several government operated centers along the coast. The main principle is to detect a ship on collision course as early as possible, to give the possibility to communicate with the ship and warn it to alter its course. If contact is not established, the approach implies to warn the installation sufficiently early, such that safe evacuation of all personnel may be completed. In addition, available resources may be used to try to establish contact with the vessel, if communication fails.

But the approach in this case assumes that the vessel does not want to collide. If on collision course, this is due to lack of knowledge, or in some cases with intent for a certain period, with a planned future course change. This approach is not correspondingly well suited if the ship is on collision course by intent. Communication is not going to change anything, nor the use of vessels or other resources to achieve physical contact. Still, the detection of a ship on collision course will imply that evacuation of personnel may be possible, if the procedures to start evacuation in a timely manner are adhered to. This will not protect the installation, though.

Keeping a small crew onboard is the most effective risk control action. It was assumed above that a small crew may be able to deactivate external control and take over control locally and mechanically. If this fails, they should at least be able to shut of power and let the ship drift until they may be able to take back control locally or assistance from shore has arrived.

A small crew would not need to be onboard al the time, the duration could be limited to where there are critical infrastructures.

If keeping a small crew onboard is infeasible, then the only option is to ensure as far as possible that there are no possibilities for hackers to gain access to the control of an autonomous unmanned ship.

Another option would be to limit the operational area of an unmanned autonomous ship for instance by limiting the available fuel stored onboard. This is to some extent used for aircrafts, although the main approach in this case is to limit the weight the aircraft is carrying. But this would be an option with some other risks. If the ship due to weather or other unforeseen events is significantly delayed, it could run out of fuel, if this is limited. If such risks are judged to be tolerable, however, it may provide an effective manner to avoid that hackers turn a ship into a threat to goals far away from the intended route. A battery powered ship will have such limitations in any case.

4.2 *Principles of prevention of threats*

If the ship is completely unmanned, it will be essential to avoid any opportunities any vulnerabilities in the control and communication systems onboard that may be used in a cyber-attack to gain control over the ship. This implies that complete control over the construction, procurement, management, operation and maintenance of autonomous ships without manning of the ship for any purpose is necessary. At all times, no unauthorized organizations nor individuals should get the opportunity to install software or hardware which may provide a "backdoor" into the control system and software available to hackers.

4.3 *Responsibilities*

Even though the probability for a cyber-attack against an unmanned autonomous ship may be low, such events cannot be ruled out in the future, and the design of autonomous ships has to involve a series of risk reducing actions and designs. Requirements to completely non-vulnerable control and communication systems may pose extreme restrictions to the construction, management, operation and maintenance of a completely unmanned ship, perhaps to the extent that the advantage of zero manning by far is overridden by costs increases associated with such restrictions.

4.3.1 *Role of ship owners*

It will be the responsibility of the ship owner who is commissioning the construction of an unmanned, autonomous ship that no alien software or hardware is allowed on board, which may be used in a cyberattack.

This will imply that every aspect of construction, procurement, management, operation and maintenance of such ships is controlled in extreme detail. All suppliers, vendors and component manufacturers and all their personnel will have to be scrutinized in order to ensure that no one has illegitimate purposes. This would be an extreme control system.

In the late 1970s, the possibility to construct nuclear power plants in Norway was considered by specialists and politicians. For a lot of the people who were against, the most fundamental argument was that there would need to be so strong requirements to control of the personnel who would operate and maintain nuclear power plants. Such very strong restrictions and surveillance of personnel were completely unacceptable to many persons.

To prevent successful cyber-attacks to autonomous ships, it will be crucial to maintain control and sufficient quality assurance over the whole software development process. This might become costly and reduce some of the expected cost savings related to autonomous ships.

4.3.2 *Role of designers and ship builders*

It is still the responsibility of designers and ship builders to implement the very strict control outlined above.

4.3.3 *Role of classification societies*

The classification societies will have to provide assurance that no alien software or hardware has been installed at any time during construction. This will require quite extreme housekeeping and control activities. It will not be sufficient to ensure that the high-quality classification societies have stringent requirements, all classification societies (high quality and low quality) need to focus on such threats.

Such assurance will need to maintained also after commissioning, due to software updates, etc. verification of software and software updates therefore becomes even more important and challenging.

4.3.4 *Role of IMO*

It is required to establish very stringent international requirements to control the risk of cyberattacks on autonomous ships. Any ship from anywhere in the world can travel international waters all over the globe and become a threat in very distant waters, provided it has sufficient amount of fuel (or operates on solar power!). All ships will therefore need to follow strict requirements.

It would be expected that the following were high-level IMO requirements for two alternative categories of autonomous ships, with and without manning:

1. Autonomous ships that always require a small crew onboard to operate
   a. Ships to have function which deactivates mechanically external control and replaces it with local control
   b. Ships to have a global power off function which as a last resort gives a dead ship
2. Autonomous ships that may operate without any crew members onboard
   a. Ships to have a function which limits the stored fuel to the distance between ports with a small margin, or
   b. Take steps to ensure fully that nobody has opportunity to install hardware or software that may be used in cyberattacks against the ship.

5 CONCLUSIONS

This article discusses cyber-attacks and its potential threat to autonomous ships. Experience from other sectors are presented and discussed. A hacked autonomous ship may be used as a weapon and ram offshore oil and gas systems, infrastructure systems along the coast, or collide with, cruise ships or oil tankers.

Infrastructure systems along the coast may be considerably more robust against collision impact compared to offshore structures. Typical offshore structures may have a resistance up to 200 MJ, which corresponds to a 5,000 tons ship with a speed of 12 knots, and are thus quite vulnerable.

Keeping a small crew onboard is the most effective risk control action, assuming that the crew may be able to deactivate external control and take over control locally and mechanically.

An option to keeping a small crew onboard is to ensure, as far as possible, that hackers cannot gain access to the control of an autonomous unmanned ship. This implies that there will have to be complete control over the construction, procurement, management, operation and maintenance of autonomous ships.

Another option would be to limit the operational area of an unmanned autonomous ship, for instance, by limiting the available fuel stored onboard. But this would be an option involving some other risk: if the ship due to weather or other unforeseen events is significantly delayed, it could run out of fuel, if this is limited. If such risks are judged to be tolerable, however, it may provide an effective manner to avoiding that hackers turn a ship into a threat for objectives far away from the intended route.

It is required to establish very stringent international requirements to control the risk of cyberattacks on autonomous ships. As ships may travel all over the globe and become a threat in very distant waters, all ships will therefore need to follow strict requirements. There will have to be different requirements to ships which require a small crew onboard than those without any crew.

REFERENCES

Advanced Autonomous Waterborne Applications (AAWA). 2016. "Remote and autonomous ships. The next steps", Position paper. http://www.rolls-royce.com/~/media/Files/R/RollsRoyce/documents/customers/marine/ship-intel/aawa-whitepaper–210616.pdf (Accessed: 2017–02–14).

Bueger, C. 2015. What is maritime security? Marine Policy 53, 159–164.

GOV.UK. 2017. Key principles of vehicle cyber security for connected and automated vehicles, guidance. Department of Transport, 6.8.2017. (Accessed: 12.11.2017: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles).

IEC61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1 – General requirements.

International Maritime Organization (IMO), Maritime Safety Committee, 2017b. Maritime Cyber Risk Management in Safety Management Systems (Resolution MSC. 428 (98)).

International Maritime Organization (IMO). 2017a. Facilitation Committee and Maritime Safety Committee. Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3, 5.7.2017).
ISO. 2011. Road vehicles—Functional safety, ISO26262:2011
Kibar, O. 2017. The car hacker (in Norwegian). Teknologi. Magasinet, Dagens Næringsliv, 5.8.2017.
Kongsberg. 2017. Autonomous ship project, key facts about Yara Birkeland. https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument
Lyche, K. 2017. The driverless car is already here (in Norwegian). Magasinet, Dagens Næringsliv, 2.9.2017.
Macher, G., Messnarz, R., Armengaud, E., Riel, A., Brenner, E., Kreiner, C. 2017. Integrated Safety and Security Development in the Automotive Domain, SAE Technical Paper 2017–01–1661, doi:10.4271/2017–01–1661.
Maritime Unmanned Navigation through Intelligence in Networks (MUNIN). D9.2. Qualitative assessment. Report, 30.9.2015.
Petroleum Safety Authority. 2017. The handling of incidents associated with ICT and information security and associated barrier management by Statoil, Audit report, PSA, 30.1.2017.
Press, G. Stopping self-driving cars from becoming cybersecurity weapons. Forbes, 19.7.2017 (Accessed: 12.11.2017: https://www.forbes.com/sites/gilpress/2017/07/19/stopping-self-driving-cars-from-becoming-cybersecurity-weapons/#4e49e2a06723)
Rødseth, Ø.J. & Tjora, Å. 2014. "A risk based approach to the design of unmanned ship control systems". In: Maritime-Port Technology and Development—Ehlers et al. (Eds), Taylor & Francis Group, London.
SAE. 2016. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, J3016_201601
Slovic, M. 2017. Security issues could still crimp the selv-driving car. Electronic Design, 28.6.2017. (Accessed: 12.1.2017: http://www.electronicdesign.com/automotive/security-issues-could-still-crimp-self-driving-car)
Statens Vegvesen. 2013. Sognefjord feasibility study floating bridge (in Norwegian only), Main report 11258–03, Statens Vegvesen, Region Vest, 15.2.2013
Statoil. 2016. Statoil's global risk management including IT Security, lecture by Monica Solem at NTNU Marin Technology Dept, October 2016
Vinnem, J.E. 2013. Offshore risk assessment, 3rd Edition, Springer, LondonUS Nayv, 2001. https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/t/terrorist-attack-on-uss-cole-background-and-issues-for-congress.html
Yu, Z. & Amdahl, J. 2018. Analysis and design of offshore tubular members against ship impacts. Marine Structures. vol. 58.