CITY, YNINERSITY OF LONDON MSc MARITIME OPERATIONS AND MANAGEMENT

MARITIME TECHNOLOGY COYRSEWORK (EPM 783)

Answer both questions below in the form of an essay written in good English. As a rough guide, answers should be about 1500 to 2000 words long but there is no absolute restriction – See General Guidance on Coursework and Examinations. Both questions carry equal marks (50).

Cyber-attack of marine systems, both on land and at sea, has become an important topic in recent years. Examine this issue and critically discuss the options available to a ship owner to reduce the risk of serious disruption to the commercial operation of the fleet. In your answer also explain the types of risk that may be encountered.

1.1 Maritime cybersecurity-main problem

Maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised

Cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders

The overall goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

Maritime cyber security, it is a problem which despite getting increasing attention, is still a major cause for concern.

Firstly the devices of ships have strong impact for cyber attack of a marine system. The Internet of things (IoT) is the internet workings of physical devices, vehicles, buildings and other items . Although the systems provide increased safety for ships, many of the systems on a ship or port are interdependent . For example, the automatic identification system (AIS) has several (in some cases up to seven) key systems dependent upon it, including radar and the chart plotter. Further, the human control of the ship and port is being reduced while the IoT plays an increasing role in ship and port governance, surveillance and monitoring systems. This increased automation and the decrease of human intervention on ships and in ports provides fertile ground for security breaches. Cybersecurity on ships and in ports now becomes of paramount importance.Security issues and potential of cyberattacks have several facets, but their economic impact on the shipping industry and port operations is huge. he maritime trade is so crucial that any obstruction in the global supply chain eventually causes catastrophic problems in both a national and the global economy. A cyberattack can mislead ship as to its direction or as to the location of the port. An uncontrolled or misled ship can interfere with essential maritime traffic in a waterway. Depending on the time the waterway is not functional and/or the amount of damage caused by the interference, critical goods may not arrive intact and on time. This lack of product supply impacts not only retail market items but also emergent needs including medicine, fuel and food. Security of the waterways may seem as merely a safety problem. However, it is much more than the safety circumstance. The side effects of disasters caused by a hacked port system or deluded on-board ship system include environmental threats. Serious damage resulting in closure of trade ways leads to complications including shifting of long-term trade and shipping routes and may require rebuilding the infrastructure such as locks and dams as well as commercially established networks. The key to security of the waterways is agility and constant paradigm shifting to outmaneuver those who do the maritime transportation system (MTS) harm. As the internet becomes more and more part of port operations and as

the internet enters all commercial ships beginning in 2017, the AIS aboard ships will be increasingly more vulnerable to cyberattacks. Ship owners and port directors will have to make decisions on cybersecurity. They must be a balance of the cost and strength of enhancement of cybersecurity with the increased complexity on the ship and in the port of these enhanced systems.A problem is one where the planning for adverse events such as a security breach is difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often difficult to recognize This problem context forces port managers and shipping companies to view decisions made on security in terms of mitigation and minimization of the extent and duration of the negative consequences associated with major disruptions. There is no ability to fully solve a wicked problem such as cybersecurity because wicked problems are multilayered and persistent. These problems represent a constellation of linked problems embedded in the fabric of multiple perceptions of the problem and potential solutions. Given the increasing frequency of cyberattacks in the maritime domain, cyber assets in need of protection first and foremost encompass:

- critical digital traffic/communication systems;
- critical information/databases;
- automated terminal and vessel systems; and
- critical infrastructures (Masala and Tsetsos, 2015).

Although the maritime industry assets have been largely mechanical with the major threat being corrosion, the maritime environment is not immune to the disruptions from digital and internet communication and technology. For example, the maritime community is not cyber resilient and has no specific guidelines or responses in place to deter or prevent a major cyberattack . The maritime legal issues as they relate to cybersecurity are complex. The advent of more automation and internet usage in the maritime environment brings a fundamental change in the way commerce is done and communication is accomplished. Acts of cyberaggression, like piracy, are carried out in an environment where jurisdiction is unclear." Attacks do not typically occur in a place (cyberspace) where a nation may have criminal jurisdiction. Further, the current

role of government tends to emphasize technological measures and awareness . International maritime law as well as country maritime regulation currently falls short of addressing cybersecurity. For example, the International Ship and Port Facility Code and the YSA Maritime Transportation Security Act of 2002 “do not make specific references to cybersecurity, which remains a major concern within the critical infrastructure of [the YSA]. Currently, there is an attempt to address industry guidelines on cybersecurity aboard ships intended to be applied by shipowners, managers and seafarer to mitigate maritime cybersecurity risk. The evolution of the automation in the maritime industry can be seen in the cyber-physical control systems, traffic control, logistics, network operations and safety management that represent the tools to keep the increasingly interconnected global economy effective, profitable and efficient

Cyber security of the entire supply chain is also a rising risk. Cybersecurity breaches in the maritime industry often cover other nefarious acts such as smuggling of drugs. Also, maritime security focus has been on terrorism and piracy and not cyberattacks. The focus on cyber has been more recent. Originating from accident investigation, safety aspects also concentrate on the infrastructure for prevention of environmental pollution and accident mitigation, such as ship collisions and vessel survivability, rather than cybersecurity for the network-operated, information and communication technology systems on which the safety systems rely. Further, insurance for these security risks is not addressed in many maritime policies.We can group the potential threats to the maritime infrastructure into five categories:

1) national governments, terrorists
2) industrial spies
3) organized crime groups,
4) hactivists (politically active hackers) and
5) hackers.

Also three navigation-critical systems have proven to be vulnerable

1) Global Navigation Satellite System (GNSS) – such as GPS.

2) Electronic Chart Display & Information System (ECDIS) – contains digital charts of ocean routes, but, when fed false information, can lead the crew to plot an erroneous course, or can lead them to believe they are on the correct course when they aren't
3) Automatic Identification System (AIS) – monitors surrounding traffic and continuously broadcasts its location and avoid collisions, but can be intercepted and modified to give inaccurate information about the ship's location, movements or identity.

The increasing practice of connecting shipboard systems to shoreside stakeholders via satellite or RF radio offers hackers opportunities to intercept and transmit falsified data, either to the ship or to stakeholders onshore. And anyone who can access system YSB ports may maliciously or unknowingly download false data or malware.

These critical systems are not the only onboard systems that are vulnerable, either. Others include cargo management systems, bridge systems, propulsion and machinery management and power control systems, communication systems, access control systems, and others.

The main issue is that with more automation there are less people available for vigilance. There have been several incidence to date including the Port of Antwerp attacks to hack systems to identify drug filled containers . The unique challenges of maritime cybersecurity include the issues with securing vessels at sea, together with the shore based infrastructure supporting this industry, in particular, the cyberattacks possible on maritime-related systems for navigation, propulsion and cargo .The Electronic Data Interchange standards exist for the individual transportation sector, but the standards are not compatible across all modes of transportation, and authentication protocols are not keeping up with the standard or threats Furthermore, pirates exploit cybersecurity weaknesses in the maritime industry . Industry is trying improve, but both state and private actors still need to address the emerging risks and vulnerabilities in a holistic manner. However, as systems are

developed for efficiency, not much focus has been on the vulnerabilities that these systems cause.

1.2 Conclusion

The transportation industry can improve cybersecurity through the common framework of risk assessment, management, and sharing experience with other stakeholders. The community approach still affords the best option. Borrowing from the financial sector, all firms should consider developing their respective cybersecurity programs in eight areas

- staff training
- cyber intelligence
- governance and risk management for cybersecurity
- cybersecurity risk assessment
- technical controls
- incident response planning
- vendor management and
- cyber insurance .

Many studies have identified cyber risk in maritime shipping, most have not taken the critical (and expensive) next step of actually identifying the vulnerabilities present in these systems.

The complexity of the systems makes them extremely vulnerable. Much emphasis has been focused on the cyber infrastructure overlooking the software vulnerability including the code and remediation measures. Generally, the most effective solutions to protecting seaport cyber infrastructure and practices does not involve new approaches or strategies, but instead focus on rigorously applying known methodologies .We should make cyber systems more resilient .An organization must :

- understand the entirety of the cyber infrastructure impacted by the organization

- establish benchmarks for the system
- measure current activity frequently again those benchmarks
- detect anomalies and
- response immediately to the anomalies detected.

We focused on:

- understanding the complex driver of risks to ports and ships
- understanding core infrastructure vulnerability of ports
- understanding the functional vulnerability of ports including broad risk elements such as workforce and other economic elements and
- addressing mitigation strategies.

Because of the sensitivities surrounding the protection of the environment it is likely that ship design will change in response to these concerns. Similarly, to cater for perturbations in the economic climate. Design in this context would typically embrace the hull, machinery, navigation and cargo handling as well as aspects such as noise emissions and levels of automation. Within these scenarios discuss within the context of dry cargo ships what the ship of the future may look like.

There is no doubt the shipping sector is experiencing a situation where considerable focus and attention are placed on environmental issues by regulators, charterers, investors, insurers, banks and, last but not least, the public and the media. Operational pollution from ships can be subdivided into two main categories: sea air pollution and water pollution. The prevention of operational sea water pollution from ships has been largely dealt with at international level over the last decades, too. The introduction of invasive marine species into new environments, by ships' ballast water or attached to ships' hulls and via other vectors, has been identified as one of the greatest threats to the world's oceans. Nisible emissions, at the start of engines or when a sudden request of power is necessary, are very difficult to control and eliminate. The black smoke, in operating conditions other than those mentioned above, may be related to the fuel quality and maintenance of engines and their exhaust. Fuel conditioning, e.g. by means of microemulsion or ultrasound or other means, could be an answer to this problem. International rules do not give detailed requirements in this regard. An example of a national standard (Alaskan Standard for passenger ships), reported in the following, gives a detailed regulatory framework in this respect. Nisible emissions, excluding condensed water vapor, may not reduce visibility through the exhaust effluent by more than 20 percent. The production of NOx depends mainly on the engine design and its operating conditions, but also on the type of fuel (for example fuel oil or LNG). According to recent studies, 33% of NOx comes from shipping and they are considered responsible for acid rains and euthrophication. Mechanisms are presently available to reduce NOx emissions such

as improved combustion, by means of specific technologies, like fuel microemulsion, charge air humidification, direct fuel injection, but, for a substantial reduction, as required by TIER III, Selective Catalytic Reduction devices are to be foreseen. It is generally recognized that a reduction of NOx emissions could be achieved by reducing the combustion temperature, but this will also reduce engine efficiency with a higher fuel consumption (to get the same power from the engine) and consequently greater CO2 emissions. The impacts, at different levels, of the new technology to be adopted, in terms of space, cost, reliability, maintainability and easy conduction by the operators is still under consideration by designers, shipyards and device manufacturers

Also mechanisms are presently available to reduce SOx emissions, without using specific low sulphur fuels, such as dry and water based type of scrubbers, in open loop (the water is taken from the sea, used for washing the exhausts and discharged, after a purification / separation process, into the sea) or in closed loop (the water is treated with additives, used for washing the exhausts, purified and processed to be ready to be reused). d processed to be ready to be reused). The amount of space needed, the additional power required, for example in the case of open loop scrubbers, the additives necessary for the correct operation of closed loop scrubbers, the weight of the dry scrubber solutions are all aspects to be carefully considered in the design of new ships and even more in the case of retrofit works to be performed on existing ships.

The Ship Energy Efficiency Management Plan is a practical tool to assist ship owners and ship operators in increasing the energy efficiency of ships in operation. The purpose of the plan is to encourage application of the many fuelsaving practices currently available. The most obvious include

- improved voyage planning (weather routing/just in time)
- speed and power optimization
- optimized ship handling (optimization of ballast, use of rudder and autopilot)
- improved fleet management
- improved cargo handling and

- on-board energy management (e.g. engine heat recovery)

Nowadays, the words “fuel saving” are used more and more in the shipping industry. The reasons are many and varied. Reduction of fuel costs, which have increased incredibly in the recent past, with an expectation of further increases, compliance with ongoing and future regulations, protection of the environment, preparedness to comply with possible future initiatives. In the fuel-saving context, two main approaches are to be considered: the design approach and the operational approach. The first, mainly related to new ships or ships undertaking significant retrofit works, the second to all ship.

Speaking about ship design, at least three concepts are to be considered: energy saving (save the energy you do not really need), energy conservation (do not waste available energy), alternative source (investigate whether or not a new energy source may be used on board). Many solutions are available and are discussed under each of the above concepts: hereinafter some examples. Energy can be saved by adopting appropriate hull forms and appendages, an air lubrication solution to reduce friction between the hull and the sea, highperformance painting (siliconic, fluor polymeric), making the correct choice of engine needed for the particular ship, installing high performance propellers, controrotating propellers, propeller inlet ducts, rudder bulbs and using high efficiency electrical users, including low consumption lights. Energy can be conserved by reducing the waste heat or using the heat available on board to generate other power, or optimizing on-board systems such as the air-conditioning plant. In the future, technological developments could lead to improving the contribution to the ship’s power needs from sources that nowadays, when used, supply only a small percentage of the total required power: wind, solar and other alternative sources.

A good environmentally designed ship but badly operated does not reach the target of minimizing its impact on the sea water, on the air and more in general on the environment. Also in this case it is useful to identify four concepts to be considered:

- energy saving (save the energy you do not need during ship operations),

- monitoring (measure important parameters: if you do not know where you are, how can you reach your target),
- maintenance (maintain performance) and
- the human factor (the most important factor to reach any target).

How to save energy during ship operations?

Among all possible choices, the following are listed only as examples:

- speed reduction and optimization,
- itinerary optimization (voyage planning),
- weather routing,

and what to measure and monitor?

- Fuel consumption using adequate tools, sensors, computer based system
- draft & trim, helping the master to keep the most efficient sailing;
- engine emissions, monitoring correct engine behavior.

Fuel saving is an ongoing process and is based on the continuous good performance of all systems involved. Maintenance of hull, propeller, engines and energy consumers is consequently of paramount importance. Who is the main actor in all this operational part of the fuel saving? Everybody on board can contribute to fuel saving. Crew environmental awareness (training) and crew motivation in respect of the ship's environmental behavior are the key factors for a successful fuel saving program. As briefly presented above, many measures to protect the marine environment are already approved and will come into force in the next few years for the reduction of NOx, SOx and CO2 emissions, others are ready to enter into force as soon as they reach the required quorum of signatory flags representing the required minimum fleet tons, such as the BWM Convention. No doubt all of them will affect the marine industry including the way to design and operate new and existing ships. Research and technological innovation will be necessary to cope with such requirements in a sustainable way.

Bibliography

Bivens, D. (2014), "Maritime governance: designed with security in mind", Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea,.

Boin, A. and McConnell, A. (2007), "Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience", Journal of Contingencies and Crisis Management.

Briefing based on the Global Sustainable Shipping Initiatives report.

BSR Sustainability Trends in the container Shipping, A Future Trends Research.

Caponi, S.L. and Belmont, K.B. (2015), "Maritime cybersecurity: a growing threat goes unanswered", Intellectual Property and Technology Law Journal.

Clancy, E., Coonrod, J., Fossati, K., Putty, S. and Sullivan, E. (2017), Interview performed in February 2017.

Csorba, J. and Husteli, N. (2014), "Securing your control systems: overcoming vulnerabilities", Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea.

Danos, A. (2014), "Building port resilience: how cyber attacks can affect critical infrastructure", Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea.

Dickman, D., Locaria, D.N. and Wool, J. (2014), "Reducing cyber risk: marine transportation system cybersecurity standards", Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea.

Evolutionary trajectory planning of ships in navigation traffic areas", Journal of Marine Science and Technology, Vol. 4.

Fitton, O., Prince, D., Germond, B. and Lacy, M. (2015), The Future of Maritime Cyber Security.

Smierzchalski, R. (1999), "Evolutionary trajectory planning of ships in navigation traffic areas", Journal of Marine Science and Technology, Vol. 4.

https://www.marineinsight.com/environment/what-is-green-ship-recycling/

https://www.marineinsight.com/green-shipping/13-technologies-to-make-the-ultimate-green-ship/

https://www.marineinsight.com/environment/what-is-green-ship-recycling/