אוניברסיטת חיפה
University of Haifa
جامعة حيفا

HMS
מרכז חיפה למחקרי מדיניות ואסטרטגיה ימית
Haifa Research Center for Maritime Policy & Strategy

# MARITIME STRATEGIC EVALUATION FOR ISRAEL 2016

Chief editor: **Prof. Shaul Chorev**
Edited and produced by: **Ehud Gonen**

# Chapter 7: The maritime aspect of cyber warfare

***Eitan Yehuda***

## General

In recent years, on top of the terrestrial, maritime, aerial and space domains there has been added an additional domain – the cybernetic domain.

Cyber attacks are very common and are perpetrated by diverse entities against a variety of organizations and systems and at all levels.[1] The attacks are perpetrated against state entities and government ministries, military entities, public and municipal infrastructures (such as electricity generation, water conveyance, municipal traffic light systems and toll roads) and also against private targets such as banks, commercial companies and private individuals.

Cyber attacks are conducted by terrorist organizations, hostile states, political activists (such as anarchist organizations and hackers) and of course by criminal elements for economic gain. Targets of the attacks may be varied and diverse; damaging or disabling computer systems, gathering information, gaining control of the computer system for ransom purposes or for the sake of perpetrating another attack in the future and in order to harm national infrastructures or public order and morale.

The means of attack are also varied and they include use of diverse transmission and infection technologies and/or use of the human factor for the purpose of inserting the software or the malicious code into the information or communication systems under attack.

In this context, the vulnerability of the port and shipping sector to cyber attacks is immense. The consequences of such an attack could be significant at a national level and accordingly it is necessary to specifically address this issue within the framework of the overall maritime strategy of Israel.

The efficacy of the ports and the quality of the vital service that they provide depend entirely on the quality of the communication, the logistics and the information systems and the technology being implemented by the port. Among these systems can be noted: perimeter defense and security systems, systems for container management and routing and for pinpointing their location, systems for

1 SYMANTECH, 2016 Internet Security Threat Report; https://www.symantec.com/security-center/threat-report

crane and derrick management, ERP systems for budget, inventory and personnel management, safety systems for communication between the ships and the ports, etc.

The shipping sector also has significant computing requirements. The ships (both the merchant ships and the passenger ships) are being built increasing larger and their operation is based entirely on advanced computing systems, such as navigation and detection systems, buoyancy control systems, loading and unloading management systems, mechanical system control (engine, generator, steering), docking systems, etc.

The growing reliance on communication (satellite and internet) based advanced computing technologies creates susceptibility of the port and shipping world to a new kind of threat; cyber attacks against ports and maritime platforms.

## Ports of Israel

The seaports of Israel are classified as critical infrastructure and they constitute the "oxygen line" of Israel. Approximately 98% of the volume of the cargo traffic to and from Israel passes through the seaports, which serve, in addition, also as a key link in the logistics chain of international commerce in the east Mediterranean region.

Modern ports and accessibility to international shipping constitute a vital layer in the Israeli economy and this due to the heavy dependence of the Israeli economy on food imports (a majority of the grains consumption in Israel), energy imports (all the crude oil) and imports of raw materials for the economy and for industry. Furthermore, many Israeli industries are dependent on overseas markets, i.e. on exportation. Any damage to the operation of the ports would cause damage to many industries in Israel, such as the Israeli chemical industry, the electronic chip export industry and additional industries.

In Israel there is 'emergency economy' (EE) preparedness, which is regulated, inter alia, under the 'Emergency Labor Services Law'. By definition of the Law, a critical enterprise' is:

> *…The enterprise operates or can be operated for purposes of defense of the State or public safety or for maintaining critical services; as well as any enterprise or part thereof that can be operated for purposes*

*of maintaining the economy and whose operations are critical for maintaining necessary supplies or services for the public or for export.*

An additional definition of the Law for a 'critical enterprise' is:

*…A service that in the Minister's opinion, if interrupted, may, in the specific circumstances, cause great economic harm that affects the economy as a whole.*[2]

The Emergency Authority does not publish the list of critical enterprises for reasons of State security, however it is clear that the ports of Israel meet the aforementioned definitions and it is reasonable to assume that they are defined as a critical enterprise and also as an enterprise rendering 'crucial services'.

Also from these emergency definitions we can infer the decisive importance of the ports to the Israeli economy.

## Risks

The dramatic developments that have occurred in recent years in communication and information technologies have affected the manner in which state actors and non-state actors operate and will operate within the maritime domain. These technologies have created opportunities, but also challenges for stakeholders in the military sphere and in the commercial sphere and also for stakeholders from the criminal and terrorism world. The sea is an enormous domain where the platforms (whether ships or other platforms) operate at a great distance from the coast; due to the complexity of these activities uninterrupted and continuous information transfer is necessary from the vessels to the coast and back. In the modern maritime domain, computer-based technologies, including guidance, sensor, control, command and communication systems, as well as linkage between the platforms of the vessels and the coastal infrastructures (such as ports) are critical for creating output and increasing efficiency.

Beyond the serious damage to the State economy or to a specific shipping company, damage to key ports or to major actors of the shipping world has the potential of damaging regional and even global trade. The global structure of the shipping industry, just as the reliance on transshipment of containers between worldwide lines and feeder lines create a situation where damage to a particular port or to a

2 Emergency Labor Services Law, 5727-1967, (Amendment No. 1) 1973-5733 (Amendment No. 7) 2008-5768.

particular company may have a global impact. For example, in 2015 27.52 million containers passed solely through the ports of Hamburg, Rotterdam and Antwerp. These containers constitute roughly 8% of the total worldwide goods traffic.[3] In the United States, the Long Beach port alone renders service to approximately 2,000 ships every year, carrying 6.7 million containers, which in turn constitute one fifth of the container traffic in all U.S. ports.[4]

From an analysis of this threat by the insurance companies, the regulators and the merchant navies there emerges the recognition of the fact that if up to now the navies were required to cope with specific incidents of cyber attack on an individual ship, then a broader attack could lead to systemic damage (damage to an entire fleet), with serious implications for global trade and for the environment.

The following is a description of some of the risks that may be caused by cyber attacks on ports, ships and energy rigs:

### Economic risks

- Damage up to disabling of work processes at ports and damage to the foreign trade of the state.
- Damage and destruction of mechanical systems of the ships up to damage to the hull itself (hitting a sandbank).
- Damage and destruction of the coastal infrastructures of the port (derricks, docks).
- Economic damage to the insurance companies and indirectly increasing premium payments by the shipping companies and rising costs of international trade.
- Disabling of critical central or regional infrastructure and damage to the global logistics chain.
- Damage to the reputation of the shipping company.
- Disabling of the processes of gas production and gas conveyance from the offshore drilling rigs, which will lead to damage to the economy due to impairment of the energy supply (gas or oil).
- Commercial smuggling that could harm the economy and public safety.

3 ENISA European Network and Information Security Agency.

4 GAO United States Accountability Office.

### Environmental risks

- Pollution of the maritime environment by oil or other hazardous substances by gaining control of oil tanker systems and deliberately colliding with a sandbank, or opening drain taps and releasing hazardous substances into the sea.
- Damage to gas rigs or to the maritime pipelines and disruption of the drilling and conveyance processes, which would cause release of hazardous substances into the sea.

### Security risks

- Damage to the national robustness of the state by disabling foreign trade for long periods of time and damage to the food and fuel supply to the civilian population and to the military.
- Remote takeover of the navigation systems of a ship and use of the ship itself as a tool for perpetrating an attack, such as 'knocking over' an oil rig or blocking a port (for example, by tampering with the data and erroneous decision making by the command crew of the vessel).
- The maritime aspects of terrorism, such as smuggling explosives and warfare materials, chemical attacks by hazardous substances, etc.
- Smuggling people by sea and illegal immigration.

Cyber attacks against ports and ships are not only a threat. Such attacks have already been perpetrated over the last year and on large scales.[5]

In 2013 a cyber attack was perpetrated on the container loading information systems at the Port of Antwerp, Belgium. For two years drug dealers gained remote control of this system and altered the content of the containers and their destinations, which enabled them to smuggle drugs in enormous quantities into the country.

A cyber attack that was perpetrated on an oil tanker off the coast of Africa caused the tanker to tilt sideways until it was completely disabled.

Somali pirates in the Gulf of Aden hired hackers in order to identify ships carrying valuable cargo, which have minimal security, in order to take control of that ships.

The national shipping company of the Islamic Republic of Iran, 'IRISL' was attacked in 2012. The attack disabled all the logistics information systems that handle control of the container movement and their location. The hackers who infiltrated

5 http://www.gard.no/web/topics/article/21025160/cyber–security

the 'IRISL' computer system deleted all the databases of the company, including the backup systems, so that the company had no recoverability from this incident.

## The situation in Israel

The State of Israel is of course preparing for the issue of defense against cyber attacks. IDF, like the rest of the defense establishment, has addressed the issue at a relatively early stage and the handling of the maritime sphere within the defense establishment has been gaining increasing attention.

A 'National Cyber Bureau' has been established in Israel, which aims to improve the protection of the critical national infrastructures and to secure them, if possible, against cyber attacks. The Bureau simultaneously promotes the status of Israel as a center for developing information technologies, while strengthening the cooperation between academia, industry, the private sector, the government ministries and the defense community.[6] The Bureau is responsible, inter alia, for coordinating the guidelines for the ports and for the coastal infrastructures in Israel.

In the civilian sphere, the legal foundation for regulation in the field is the 'Regulation of Security in Public Bodies Law, 5758-1998.[7] The Law prescribes authorities and responsibility for physical security, information security and critical computer system security in various bodies, including all the ports in Israel (both Israel Ports Company ports and Eilat pipeline and Israel Electric Corporation ports and marinas), as well as the shipping, energy and gas companies. Among other things, the law requires the appointment of a 'security officer' in the foregoing bodies, under the guidance of the General Security Services or the police, depending on the body in question. The authority of said officer includes providing professional guidelines on security issues, information security and critical computer system security in each one of the various bodies.[8]

The statistical yearbook published by the Administration for Shipping and Ports (ASP),[9] describes in detail the Administration's duties and the importance of

6 National Cyber Bureau, Prime Minister's Office. http://www.pmo.gov.il/BranchesAndUnits/Cyber/Pages/NationalCyber.aspx

7 Regulation of Security in Public Bodies Law, 5758-1998: https://www.nevo.co.il/law_html/Law01/111M1_001.htm

8 Regulation of Security in Public Bodies Law, 5758-1998. First Schedule Order 5766–2006, Order (No. 2) 5776-2016.

9 ASP Statistical Yearbook for 2015 (published March 2016). http://asp.mot.gov.il/he/abstract

the seaports to the commercial processes of the State of Israel, Among other things, it is written in the yearbook that: "It can be summarized and said that the economic future of the State of Israel largely depends on development of the ports, on creating conditions for competition between the domestic and foreign users thereof and on increasing their efficiency."

On the area of information systems and technologies the following subjects appear:

- Establishment and operation of information systems for shipping and ports.
- Establishment of a national shipping and ports database.
- Uniformity in the computing infrastructures at the ports.
- Regular collection, processing and dissemination of shipping data.

Nonetheless, there is no mention at all of the subject of coping with cyber threats on the information systems and the communication of Israeli ports and Israeli shipping companies, this despite the importance of this subject and the guidelines provided under the law.

The operational and legal structure of the shipping world is highly complex due to the global spread of the shipping lines; the ports and the coastal infrastructures being under the sovereignty of different states (and therefore, their being subject to non-uniform laws, regulation and ordinances); the registration of many ships under flags of convenience, etc. Therefore, in general it is possible to differentiate between three principal levels of analysis: The level of the state and its costal infrastructures; the international level; and the level of the shipping company. These three levels are naturally influenced by one another and sometimes even overlap.

**The coastal infrastructure and port level** – this is of course national infrastructure under the complete sovereignty of the coastal state, which can also prescribe mandatory cyber regulation for the port. Nonetheless, it should be taken into account that the communication infrastructures of the port must adapt 'and speak' with many ships, which are bound by different standards, depending on their country of registry. Increased rigorousness in the cyber communication sphere could deny the port the ability to communicate with the ships effectively. The regulations prescribed by the coastal state are usually derived from the international requirements in the sphere, which constitute 'minimum requirements'. Nonetheless – just as in the Israeli case on the cyber issue – the state can prescribe stricter and tighter regulation for its coastal infrastructures and ports than the world standard.

In January 2015, the auditing body of the U.S. Congress (Government Accountability Office – GAO) published a report on the subject of cyber in U.S. ports. According to the report, the U.S. ports handle annually cargo valued upwards of $1.3 trillion. All this activity is supported by information and communication systems that are susceptible to cyber attacks. Failures in these systems could harm or disrupt the port activity and including the flow of commerce. The report's recommendations are that the Department of Homeland Security should direct the coast guard to assess the risks pertaining to cyber attacks and use this assessment in order to assist in developing security guidelines for the maritime sector as a whole. Moreover, the report recommends re-establishment of the cyber threat coordination council in this sector.

**The international level** – currently different states have international commitments to international treaties and to international codes. Furthermore, implicitly or explicitly, each one of the states is committed to an operating practice derived from the requirements of major actors in the sphere, such as the major insurance companies, etc.

Among the major insurance companies growing interest has been noted on the subject of cyber attacks. Once a year, the global insurance company Allianze publishes a report that surveys the losses and the security level of the shipping world around the world. An analysis of the most recent report[10] reveals that the first reference to awareness of the subject was published only in 2013 and that since then there has been no serious progress on the subject. The most recent report defined the cyber world as one of 'the significant threats' to the shipping world and primarily to the navigation systems (GPS), to the command and control systems (Electronic Chart Display – ECDIS) and to the automatic identification systems (Automatic Identification System – AIS). It should be emphasized that the aforementioned systems are linked to the internet world and to the external communication systems and that any damage to them could result in significant financial losses and insurance claims.

Last February, the world shipping association, which represents more than 2,200 ship owners (Baltic and International Maritime Council – BIMCO), published a guidance document for ship owners and their operators under the title The Guidelines on Cyber Security Onboard Ships.[11] The guidelines describe how to

10 http://www.agcs.allianz.com/insights/white-papers-and-case-studies/safety-and-shipping-review-2016/

11 https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf

prepare against the new threat. BIMCO claims that understanding of the threat should begin at the senior management level and not remain the province of computer personnel only. The document notes that all the systems on the ship and at the ports that are based on advanced computer technologies are vulnerable to cyber attacks, including the internet networks intended for the well-being of the crew members and of the passengers on passenger ships. Within the report a mapping was made of all the systems and it includes an in-depth analysis of the degree of potential damage that could be caused as a result of damage to them and recommendations on actions that crew members should take in the event that these systems are disabled. The main recommendation of the report is to conduct a risk analysis and to create a disaster recovery plan.

If we take, as a case study, the threat of piracy attacks in the East Africa region, it appears that the stakeholder shipping companies and states have invested vast resources in order to combat the phenomenon. Over time, and with refinement of the piracy activity, the shipping companies and the insurance companies have begun to take precautionary and protective measures in order to reduce and neutralize the risk. The major factor affecting the considerable decline in piracy activity in this region is attributed to activity of the UN international maritime task force, in which twenty two states are members. As stated, guidelines for preventive behavior, for communication and for reporting have been disseminated among the various forces and organizations operating within the domain in the event of an attack. Concurrently, there has been a rise in the number of private security companies providing a local response for the shipping companies. As a result of this extensive activity, the number of piracy attacks in the East Africa region has declined to a negligible level. This example illustrates the discrepancy between providing a response to a real and tangible threat and the cybernetic cyber threat, which is not tangible and therefore the appropriate management resources and budgets are not being invested there, despite the significant danger that it poses.

**The shipping company** – the decline in the maritime transport costs and the significant erosion of profits in the maritime freight sphere (ZIM for example presented in the most recent reports of 2015 a half-yearly loss of $132 million) have made it economically difficult for the shipping companies to invest in advanced information security technologies and prompt them to take big risks.

Here are a few of the challenges with which the shipping companies are forced to deal in this sphere:

- The life cycle of technological systems and the large number of hardware and software manufacturers for vessels causes rapid obsolescence of the operating systems and this before having to replace all the systems and facilitates hacking into the systems.
- The communication between the ports and the ships is based on an open not encrypted medium, which aims to save the costs of upgrading the systems to encrypted systems.
- Development of the systems and the software at the ports and on the vessels was not done under a 'secure development' concept and now an enormous investment is required in order to implement a conversion to this concept.
- A lack of skilled professionals in the field.

Unlike other areas in the world of ports and shipping, such as shipping safety and environmental protection, there is currently no regulation or clear and mandatory guidelines. Therefore, cyber security is subject to local initiative of the shipping companies without a mandatory national or international directive.

## Summary and recommendations

The ports of Israel constitute the oxygen line through which roughly 98% of the volume of goods comes to Israel. Therefore, it is advisable to give consideration to adequate protection against the new cybernetic threat facing the port and shipping sector.

An analysis of the activity in Israel and around the world reveals that the entities involved in the sphere of shipping and ports (states, insurance companies, shipping associations) are aware of the cyber threat issue, but this awareness has not yet reached a maturity with the power to prompt concrete systemic steps that would cope with the threat and this contrary to what has been done in the financial or defense world.

Since the ports of Israel are a critical national infrastructure they must be protected accordingly in order to enable functional continuity. The establishment of an adequate defense array with the power to cope with cyber attacks must be part of a strategic plan that will include the following subjects:

- Determination and validation of the threat reference of the port and shipping array; this topic must be included in the outline of threats to critical infrastructures in the State of Israel.

- A risk assessment for all the systems and work processes in the port and shipping array.
- Ranking of the risks according to their degree of impact on damage to the main work processes at the ports.
- Appointment of a central body that would lead the issue and provide government entities with an analysis of the threats and recommendations for coping with each one of these threats. The body shall have the authority to give mandatory guidelines to ASP.[12]
- Defining mandatory cyber defense standards for all the ports in Israel.
- Conducting annual scheduled attack drills and surprise drills that are to be conducted by a 'red' team of the national cyber authority in order to test the efficacy of the defense.
- Classification of some of the critical information systems of the port array as core systems and development of these core systems under a concept of 'secure development'.
- Encrypting the information that will be defined as classified and of security importance to the state, as well as the communication medium between the ports and the ships.
- Cooperation with states and relevant international shipping associations in order to achieve mutual signature of information transfer agreements.
- Guidance of a national process of creating cyber standardization for the shipping world will be carried out jointly with a group of friendly and relevant states; this guidance will also help the Israeli companies in the sphere.
- This standardization will define the optimal defense response of each ship and the standardization with which it must comply in order to maintain its operational fitness and this similar to procedures that define boating safety.

Since there is continual erosion of the maritime freight prices and a significant decline in profits of the companies, we are witnessing diminishing investment in new technologies, including cyber defense systems, which constitute overhead and do not add to the operational capability of the vessels. The standardization requirement in the sphere may actually come from the side of the insurance companies and the shipping associations, which classify the cyber threat as a significant threat and regard it as a high risk component.

12 The Haifa Center for Maritime Strategy will assist the entity to be determined in analyzing the threats and recommendations with respect to solutions.

Recommendations:

- Performance of a risk analysis for the computing and operations systems and creation of a functional continuity plan during failure in one of these systems.
- Analysis of the work processes of the vessels while sailing and primarily at the port and this in order to identify primary potential failure points that would enable cyber hacking (such as the remote maintenance process of such system or another on the ship, container loading and unloading processes and so on).
- Mapping of all the systems, in terms of the software and hardware versions, and receiving security updates from the manufacturers.
- Analysis of all the means of communication that the ship has at sea and in port and establishment of an appropriate defense response (such as encryption of the communication medium, blocking devices, etc.)
- Training, exercising and drilling of the ship crew, starting from the level of awareness of the cyber threat (for example, refraining from insertion of external devices, connection between network types, proper work on the internet) and up to modes of conduct when a cyber threat is identified and the ways to contain such incident.
- Creation of a security envelope for the crew members on the ship, which includes individual inspections for key personnel that have access to sensitive systems damage to which could have disastrous consequences.

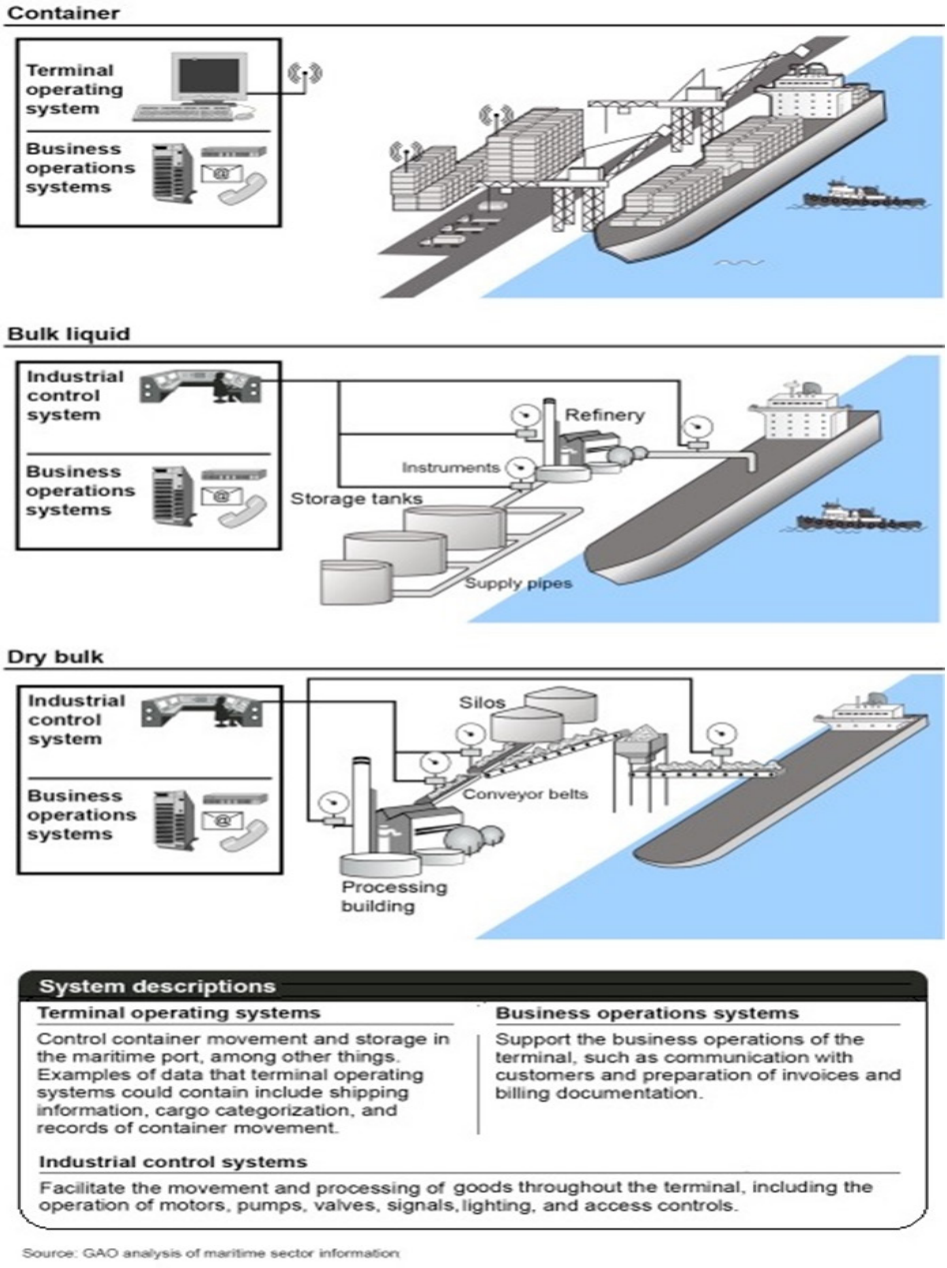


Figure 7.1 Computerized systems for communication between ship and dock

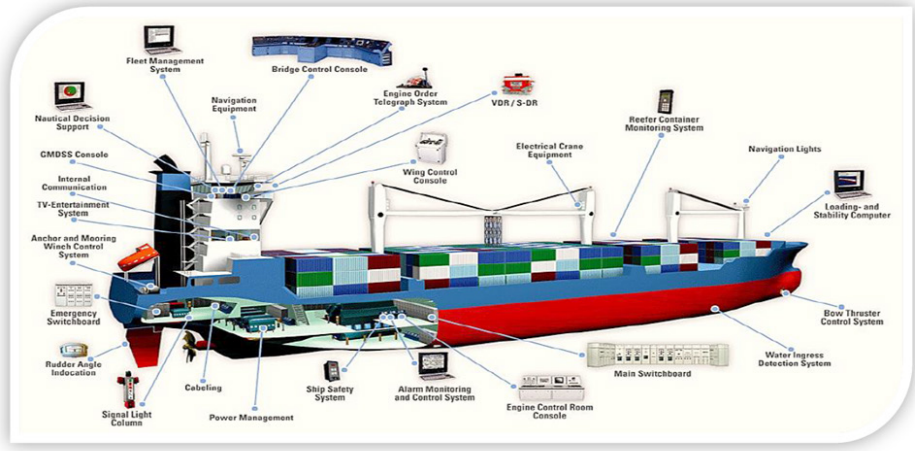


Figure 7.2 Computer-based ship systems


Figure 7.3 Port information systems