Evalution of New Risk Category: Maritime Cyber Threats

A. Tuğsan İşiaçık Çolak
Cap. Lecturer Istanbul Technical University Maritime Faculty, PhD (cont.)

Maritime Terrorism

According to the Council for Security Cooperation in the Asia Pacific, *Maritime Terrorism* is defined as, "…the undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities "

Is ISPS enough?

Since Code was adopted supporters of the ISPS Code argue that it has been successful, as no serious incidents of maritime terrorism have occurred since it was implemented but opponents argue that the code has been little to no help in protecting vessels and seafarers against modern-day piracy.

Below figures and tables show all piracy and armed robbery incidents reports to IMB Piracy Reporting Centre during 2016

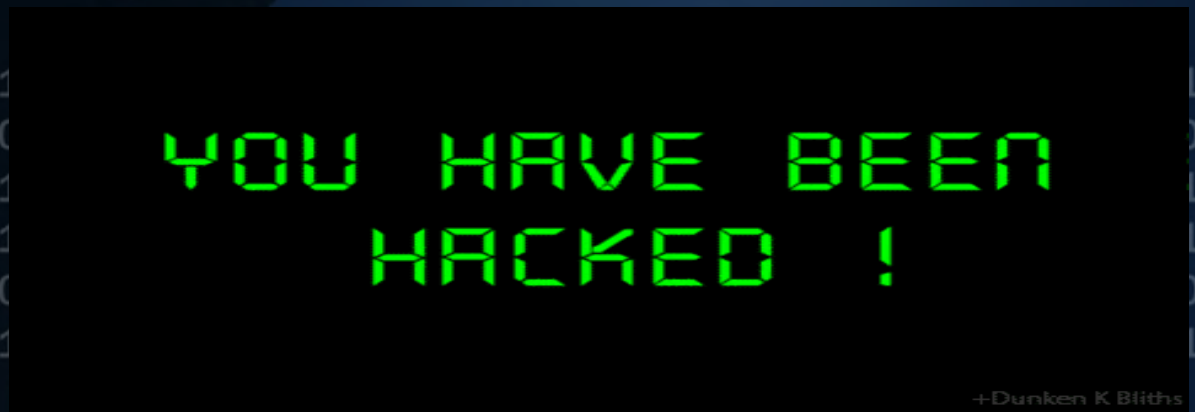
Annual Report Locations of actual and attemptedattacks during 2016

	Location	2012	2013	2014	2015	2016
S E ASIA	Indonesia	81	106	100	108	49
	Malacca Straits	2	1	1	5	
	Malaysia	12	9	24	13	7
	Philippines	3	3	6	11	10
	Singapore Straits	6	9	8	9	2
	Thailand			2	1	
EAST ASIA	China	1			4	7
	South China Sea	2	4	1		
	Vietnam	4	9	7	27	9
INDIAN SUB	Bangladesh	11	12	21	11	3
CONTINENT	India	8	14	13	13	14
SOUTH AMERICA	Brazil	1	1	1		
	Colombia	5	7	2	5	4
	Costa Rica	1				
	Dominican Republic	1	1			
	Ecuador	4	3			
	Guyana		2	1		2
	Haiti	2			2	4
	Mexico					1
	Peru	3	4			11
	Venezuela			1	1	5
AFRICA	Algeria	1				
	Angola			1		2
	Benin	2				1
	Cameroon	1		1	1	
	Dem. Republic of Congo	2		1	3	2
	Dem. Rep. of Sao Tome & Principe			1		
	Egypt	7	7		1	
	Gabon		2	1		
	Ghana	2	1	4	2	3
	Guinea	3	1		3	3
	Gulf of Aden*	13	6	4		1
	Ivory Coast	5	4	3	1	1
	Kenya	1	1		2	2
	Liberia			1	2	
	Mauritania		1			
	Morocco		1	1		1
	Mozambique	2	2	1	1	1
	Nigeria	27	31	18	14	36
	Red Sea*	13	2	4		
	Sierra Leone	1	2	1		
	Somalia*	49	7	3		1
	South Africa					1
	Tanzania	2	1	1		
	The Congo	4	3	7	5	6
	Togo	15	7	2		1
REST OF	Oman			2		
WORLD	Papua New Guinea				1	
	Yemen					1
	Total at year end	297	264	245	246	191

A total of 191 incidents of piracy and armed robbery aganist ships was reported to the IMB PRC in 2016. This is the lowest annual figure since 1998 but the number of crew kidnapped in 2016 was the highest.

(Source IMB Piracy Reporting Centre)

Maritime Cyber Threats

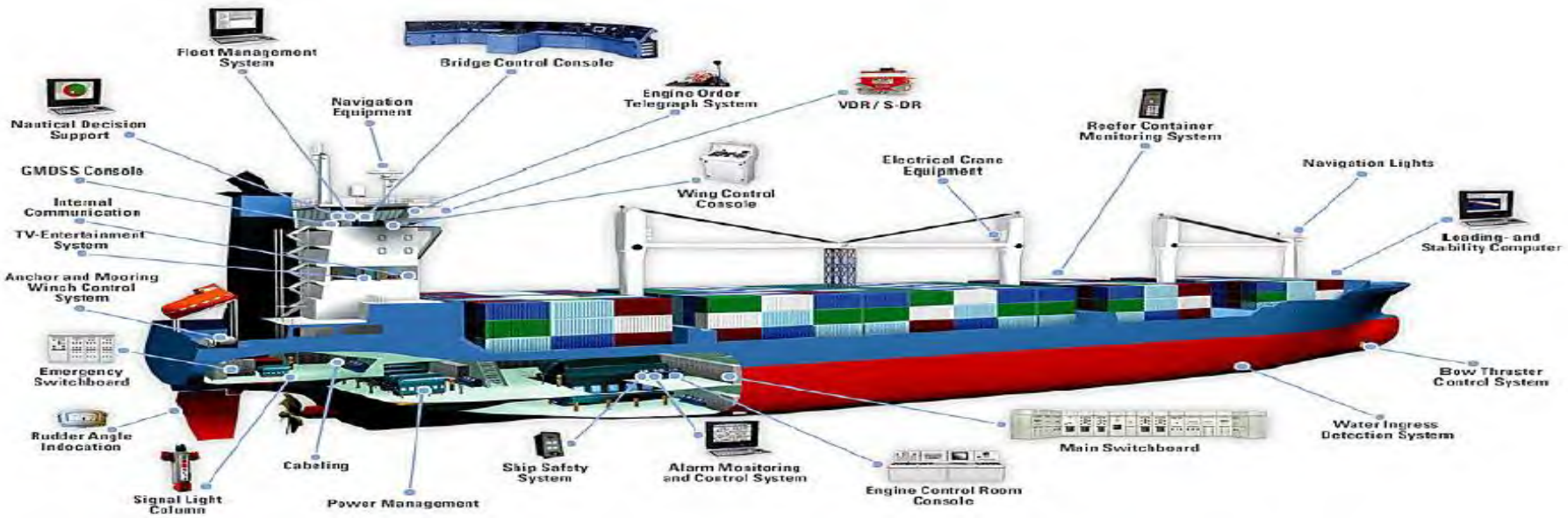


Today, cyber related risks are unquestionably a large and rapidly growing portion of all the risks ports, facilities, and vessels face.

Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment.

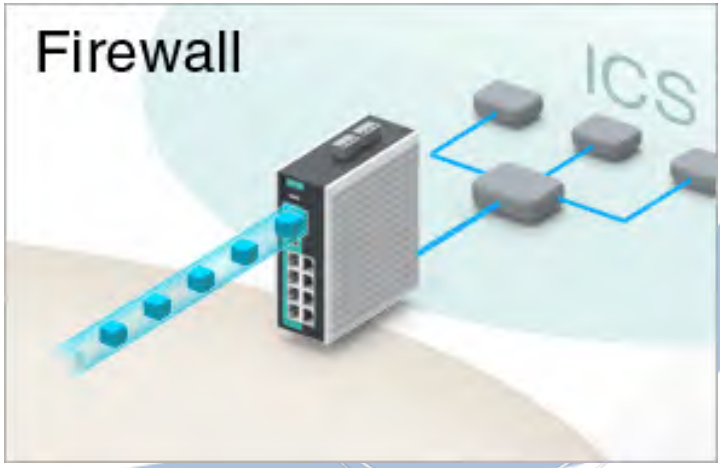
. Vulnerable systems (but not limited to):

- Bridge systems,
- Cargo handling and management systems,
- Propulsion and machinery management and power control systems,
- Access control systems,
- Passenger servicing and management systems,
- Communication systems



Defining Maritime Cybersecurity

Maritime cybersecurity as measures taken to protect network and computer assets both on ships, terminals, ports, and all computerized equipment supporting maritime operations.



A cyber-attack is any "attempt to damage, disrupt, or gain unauthorized access to a computer system, or electronic communications network.”
Cyber-attacks pertain to the same computer assets on ships,terminals, ports, and all computerized equipment supporting maritime operations.

In general, there are two categories of cyber attacks which may affect companies and ships :

- Untargeted attacks, where a company or a ship's systems and data are one of many potential targets; or
- Targetted attacks, where a company or a ship's systems and data are the intended target

Examples of some tools and techniques :

Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate known vulnerabilities in a company and onboard a ship.

Social engineering: A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.

Phishing: Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that an individual visits a fake website using a hyperlink included in the email.

Water holing:
Establishing a fake website or compromising a genuine website in order to exploit visitors.

BE WISE TO WHAT LIES INSIDE

Be cautious using removable media,
don't give your ship a virus!

KEEP YOUR P@55WORD5 LONG & STRONG

Simple passwords can be unlocked easily, keep yours long and strong.
Change your passwords regularly.

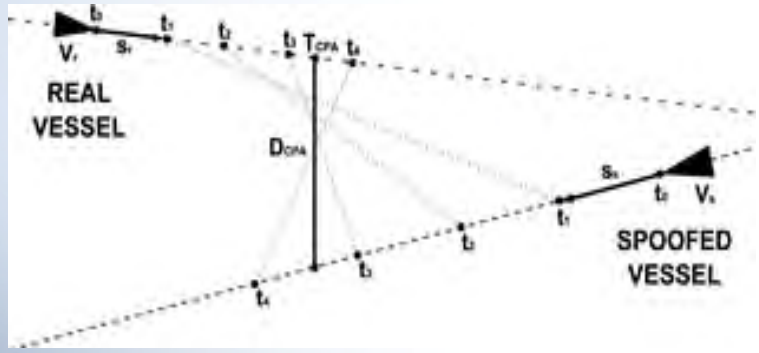
Equipment Vulnerabilities On Board Systems

Other equipments vulnerable to cyberattacks are navigation systems:

- Automatic Identification System (AIS),
- Global Positioning System (GPS),
- Electronic Chart Display Information System (ECDIS).

Because AIS doesn't have an inbuilt mechanism to encrypt or authenticate signals, AIS is considered to be a soft target for cyber-attack. Threats that affected AIS implementation are:

RF-Based AIS Threats: CPA SPOOFING: Collision avoidance is one of the primary objectives of using AIS, especially in open sea. CPA spoofing involves faking a possible collision with a target ship. This will trigger a CPA alert, which could lead the target off course to hit a rock or run aground during low tide.



Fake CPA alert

AIS-SART Spoofing. AIS-SART spoofing involves generating false distress beacons for men who have fallen overboard in specially chosen coordinates by attackers. AIS transponders are required to generate alerts when they receive distress messages. Attacker (e.g., pirates) can trigger SART alerts to lure victims into navigating to hostile and attacker-controlled sea spaces.

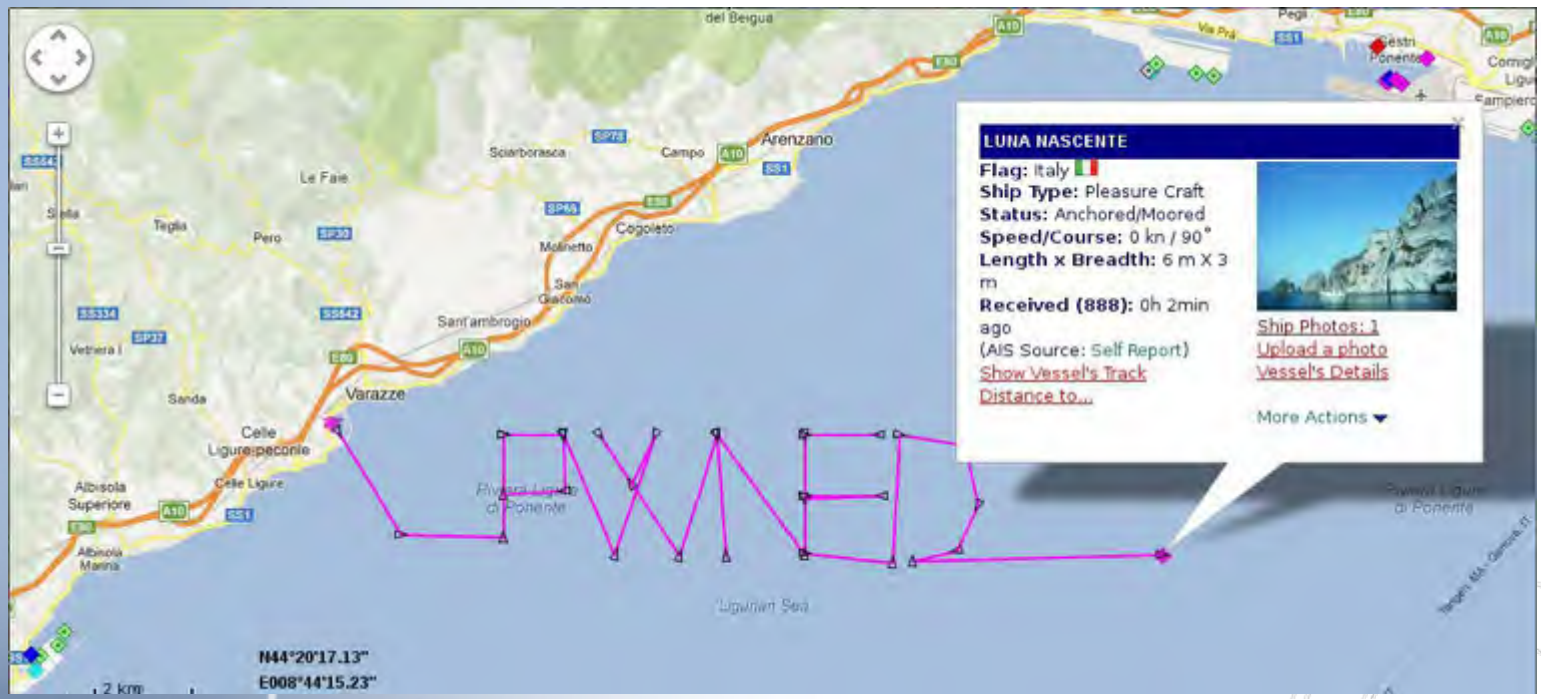
Slot Starvation: This involves impersonating maritime authorities to reserve the entire AIS transmission "address space" in order to prevent all stations within coverage from communicating with one another.

Malicious users can instruct AIS transponders to delay transmission times by simply renewing commands, thus preventing further communications about vessels' positions. This allows vessels to "disappear" from AIS-enabled radars

Ship Spoofing : Ship spoofing refers to the process of crafting a valid but nonexistent ship. It involves assigning static information such as vessel name, identifiers (i.e., MMSI and call sign), flag, ship type (e.g., cargo), manufacturer, and dimensions as well as dynamic information such as ship status (e.g., underway or anchored), position, speed, course, and destination to the fictitious ship.

Ship spoofing provides attackers a wide range of malicious attack scenarios to play with.

Spoofed ship following a programmed path



Case Study 1

Reuters exposed the illegal transportation of Iranian crude oil from Iran to China, India, and South Korea. Research exposed there were at least three Iranian ships flying a Tanzanian flag while pretending to be Syrian-owned in an attempt to avoid a boarding and inspection. Getting around international sanctions was easy for the Iranian oil company, which falsified its AIS data to reflect that of a Tanzanian ship. When questioned, officials representing the flagging agency in Tanzania denied these Iranian vessels as part of their registry. The amount of illegal oil or other goods transported by these ships is unknown and exposes another weakness in technology on which the maritime industry relies.

Case Study 2 Vessel navigation controlled by hackers

In July 2013 a research team from the University of Texas managed to take control of the navigational systems of an 80 million dollar 210-foot yacht in the Mediterranean. They accomplished this using equipment, which cost only 3000 USD to build. Essentially they injected their own radio signals into the vessel's GPS antennas, which enabled them to steer the vessel as they saw fit. Whilst they were doing this, the vessel's GPS systems reported that the vessel was moving steadily in a straight line, with no indications of changes. ".

Port of Antwerp used for drug smuggling

In late 2013 it was made public that the Port of Antwerp had been subjected to a persistent cyber attack, which had been ongoing since June 2011. The penetration allowed the attackers to have remote access to the terminal systems, and thereby they were able to release containers to their own truckers without knowledge of the port or the shipping line. Furthermore, the access to port systems was used to delete information as to the existence of the container after the fact.

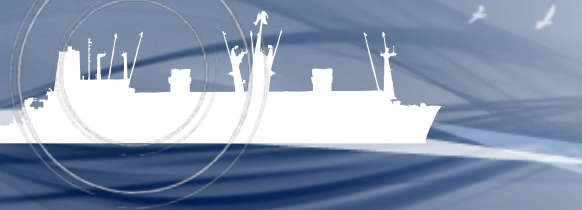
When the operation was uncovered, Belgian and Dutch police found a ton of cocaine, guns as well as more than 1.3 million Euro in a suitcase. But given the operation had been ongoing for 2 years. (this might only be a fraction of the true scale of the operation.)

Using containers as a vehicle for the smuggling operations, is certainly nothing new. However the method is clearly new and exposed what can best be described as "ghost shipping".

Attacks on offshore installations In 2010 a drilling rig was being moved at sea from its construction site in South Korea towards South America. Its critical control systems became infected with malicious software to such a degree that it had to shut down for 19 days in order to clear the issue.

GPS jamming

The UK and Irish General Lighthouse Authority performed a test on a vessel, the Pole Star8. Powerful GPS jamming equipment was directed a specific patch of ocean and a vessel was sailed into the zone to record developments. As the vessel entered the jamming zone a range of services failed: the vessel's DGPS receivers, the AIS transponder, the dynamic positioning system, the ship's gyro calibration system and the digital selective calling system.



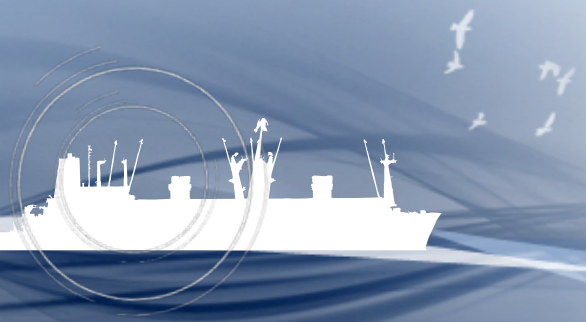
The ability to manipulate ECDIS data

ECDIS is interconnected with a wide range of other systems and sensors such as radar, Navigational Telex (NAVTEX), AIS, Sailing Directions, Position Fixing, Speed Log, Echo Sounder, anemometer, and fathometer. These sensor feeds are often connected to the shipboard network, which in turn has a gateway to the Internet.

Navigational charts are either downloaded on to ECDIS directly via the Internet or loaded from CD/DVD or USB memory disk manually by the personnel. NCC Group tested an ECDIS product to see whether penetration of the system was possible. Several security weaknesses were found including the ability to read, download, replace or delete any file stored on the machine hosting ECDIS.

Conclusion -1

The best encryption algorithms in the world are useless if someone writes the password on a Post-it note and leaves the door open.



Cyber Security occurs on 3 basic elements.

1. Technology
2. Staff
3. Processes

For technology, the virtual maritime area is protected by the device and countermeasure systems. In this respect, it is necessary to construct a kind of security wall for counter-RF technologies and ships. This can be called Maritime Universal Security Firewall or Universal Maritime Threat Management System.

All operational systems of the ship, whether SCADA or ICT, must be designed separately from the normal IT (information technology) network of the ship. These two areas are separated by the security wall.

The position of the ship must be confirmed with other INS systems on board to prevent AIS counter systems and GPS spoofers. In addition, security will be ensured through the collective position test message (including the position where the positions can be controlled by sending a position on the radar over a AIS message) to be included in the other vessel's AIS.

The human factor is the other delicate thing over there. There is a very important information security standard called ISO 27001. It is necessary to ensure that all ship personnel receive this ISO 27001 standard training. It is very important to talk about these operational cyber attacks that could damage the ship. In addition to this, training should include information technologies basicly. These training will create a cyber security awareness on board.

Conclusion -2

To mitigate against the ‘Cyber Risk’ the most vital step is to familiarise maritime cyber security and to increase cyber awareness in the Maritime Industry.

Thank you

Now, ARE WE READY FOR AUTONOMOUS SHIPS ?

References:
1. Conference of Contracting Governments to The International Convention for The Safety of Life at Sea Consideration and Adoption of ISPS Code Consideratıon and Adoption of The Resolutions and Recommendations and Related Matters SOLAS/CONF.5/34 17 December 2002
2. http://cimsec.org/isps-code-maritime-terrorism/12098
3. http://www.marineinsight.com/marine-safety/9-types-of-maritime-crimes/
4. http://www.marineeducationtextbooks.com/blog/ISPS-Code-Yesterday-and-Today
5. http://www.iacpcybercenter.org/news/cyber-risks-in-the-marine-transportation-system-the-u-s-coast-guard-approach/#sthash.CgOgmOlk.dpuf
6. https://www.uscg.mil/.../USCG_Paper_MTS_CyberRisks.pdf
7. Interim Guidelines On Maritime Cyber Risk Management MSC.1/Circ.1526 1 June 2016
8. Draft Guidelines On Maritime Cyber Risk Management MSC 96/WP.9 Annex 2
9. Maritime Cybersecurity: The Future Of National Security,Christopher R Hayes, Naval Postgraduate School, Monterey, CA
10.http://www.maritime-executive.com/article/shipping-industrys-own-cyber-security-guidelines-released
11.http://www.gard.no/web/updates/content/22140110/cyber-security-awareness-in-the-maritime-industry
12. A Security Evaluation of AIS Automated Identification System Marco Balduzzi Alessandro Pasta Kyle Wilhoit makale
13. A Security Evaluation of AIS Marco Balduzzi and Kyle Wilhoit, Trend Micro, Texas, USA,2014