Deloitte.

Cyber Security in the shipping industry

Capital Link Cyprus Shipping Forum

“We are vulnerable in the military and in our governments, but I think we're most vulnerable to cyber attacks commercially. This challenge is going to significantly increase. It's not going to go away.”

Michael Mullen - US Navy Admiral
Chairman of the Joint Chiefs of Staff

Maritime is not an exception

Hacking Ships: Maritime Shipping Industry at Risk

March 31, 2015 By Pierluigi Paganini

G+1 22 My Page Like 136

Modern maritime ships are considered a privileged target for hackers and pirates that are increasing their pressure on the Maritime Shipping Industry.

Hackers target Cyber Attack on Ships: Maritime Shipping Industry at Risk

Modern maritime ships are often monitored and controlled remotely from shore-based facilities thousands of miles away to ensure efficiency. This creates a new platform for hackers and pirates to conduct targeted cyber attacks on ships

Recent Cyber Attacks Highlight Bunker Industry Vulnerability

Monday October 13, 2014 Tweet Follow @shipandbunker

Students Take Control of $80 Million Superyacht Using Fake GPS Signals

Hey—Texas did something smart!¹² By sending fake GPS data to a superyacht's navigation system, University of Texas students were able to override the actual GPS signals and send an $80 million ship veering off course without rousing any suspicions whatsoever.

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber -attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking

UNIVERSITY OF TEXAS TEAM HIJACKS $80 MILLION YACHT WITH CHEAP GPS SPOOFING GEAR

Cyber Attack Targets Tankers

By MarEx 2015-05-20 04:46:23

IT company Panda Security has released *Operation Oil Tanker: The Phantom Menace*, a report that details a malicious and largely unknown targeted attack on oil tankers.

First discovered by Panda Security in January 2014, the ongoing attack on oil cargos began in August 2013 and is designed to steal information and credentials for defrauding oil brokers.

Despite having been compromised by this cyber-attack, which Panda has dubbed "The Phantom Menace", none of the dozens of affected companies have been willing to report the invasion and risk global attention for vulnerabilities in their IT security networks.

Maritime Shipping No Longer Immune to Cyber Attacks, Security Breaches

By: Maritime Executive
April 25, 2016

We live in a digital world that is evolving at breakneck speed. Unfortunately, rapid change can bring problems, issues and chaos, and the maritime world is not exempt evolution.

dern ships have become ever more complex l automated over the past four decades. In 1970s, most of the equipment was analog

Plenty of phish in the sea

Published on June 15, 2015 by David Rider · No Comments

Shipping industry again warned of cyber threat.

Plenty of phish in the sea

Advancement in broadband technologies and the move towards 'Big Data' will leave the maritime industry vulnerable to cyber-crime unless it develops a better awareness of ICT security and adopts security best practice, warns ESC Global Security's head of cyber security division, Joseph Carson.

Maxwell Cooter
February 13, 2015

Royal Navy under threat from cyber-attacks

Share this article:

The Royal Navy is under an increasing danger of cy up training to deal with the threat.

That's according to a report from researchers at the University of Lancaster who found that maritime systems were especially susceptible to computer attacks and that ageing systems and a lack of training were particular barriers.

Security consultant Brian Honan said that all navies, indeed all shipping companies, were vulnerable to these threats. "What the report highlights is that many ships use Windows XP or Windows Server 2003 – one of which Microsoft has stopped supporting, and one Microsoft is about to stop supporting. And because ships are at sea a lo systems. It's a problem faced by private companies too," he produced in the autumn of last year by ENISA that also poi

According to the Lancaster report, Cyber Operations in the target for cyber-criminals as 95 percent of goods are conve

GIZMODO

Ships Have Black Boxes—And Apparently, They're a Cinch to Hack

Voice, navigation, and radar data aboard ships are all at risk, according to an expert who claims that some devices that contain sensitive ship information just aren't secure enough. This could be good news for pirates and spies, and bad news for the good guys.

Deloitte.

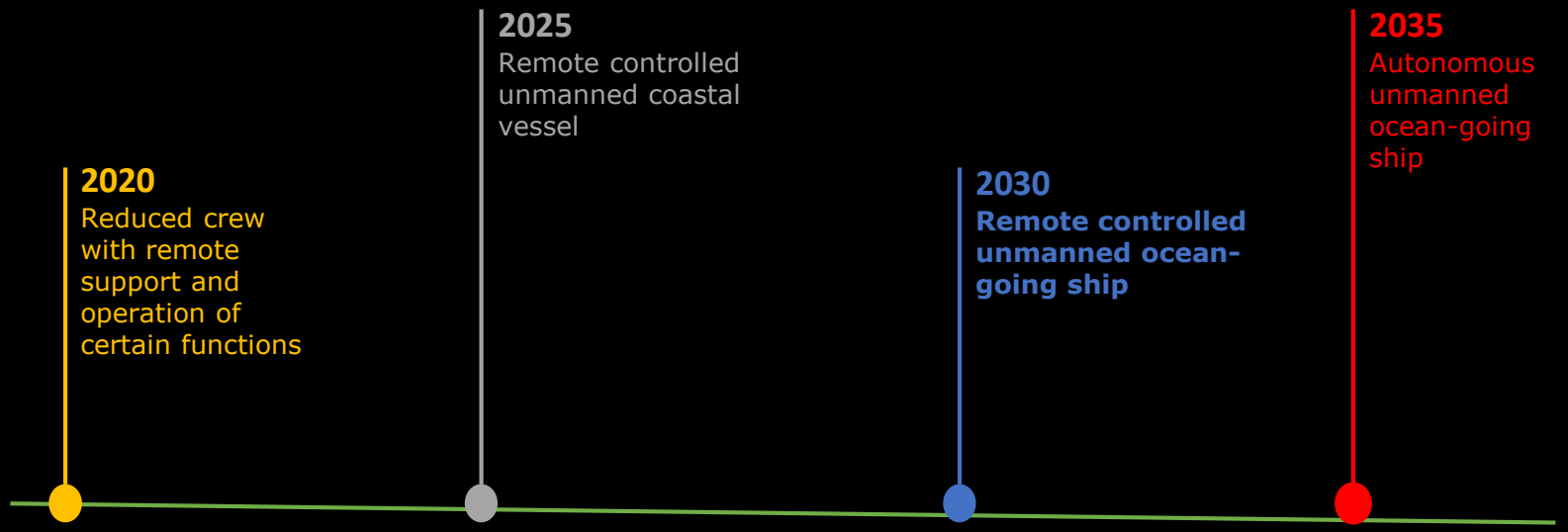
Vessel Digitization

Transforming the shipping industry

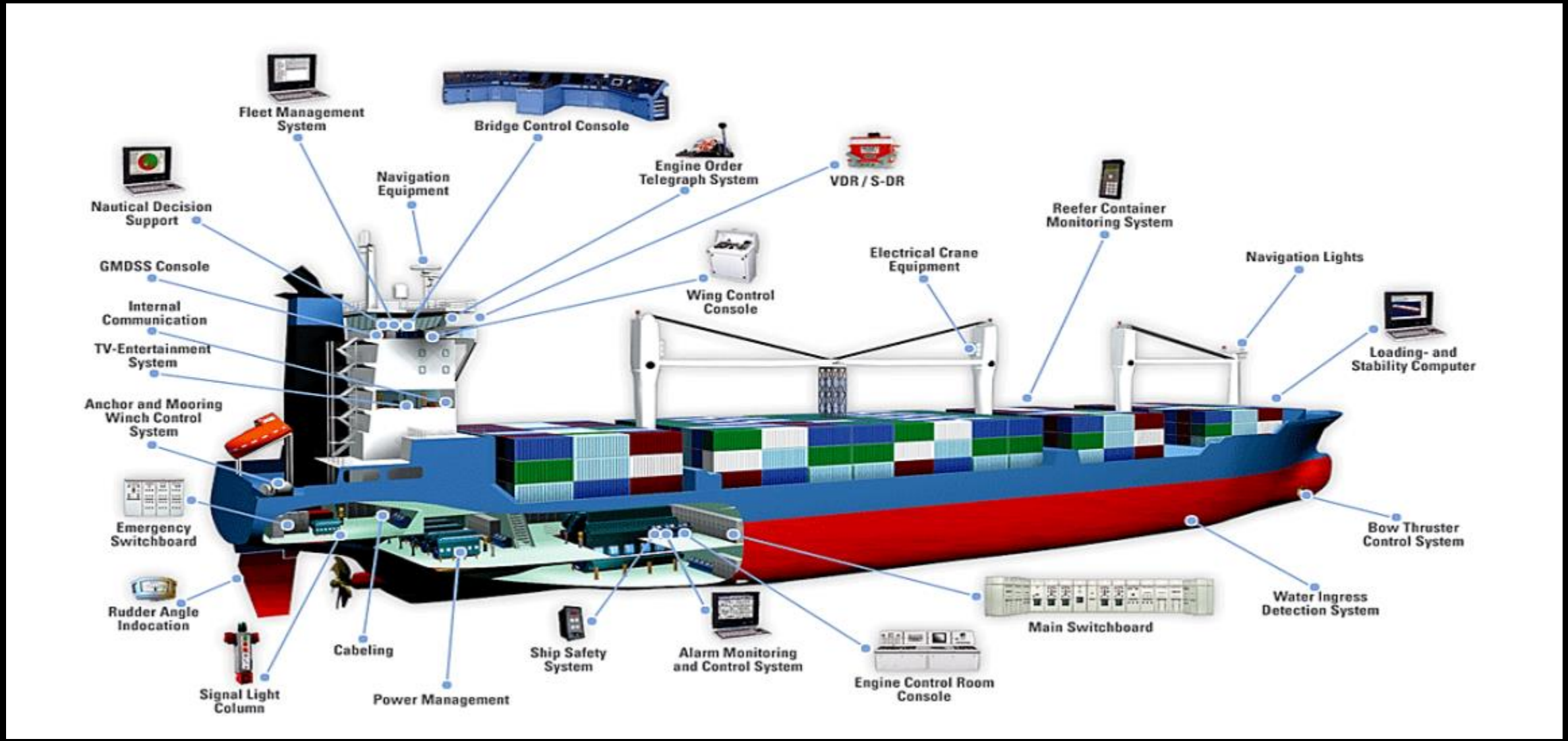
Entering the digitization era

- Computerized systems will transform the shipping industry
- Smart – autonomous or even automated ships

Rolls Royce already entered the game with the Autonomous Waterborne Applications Initiative (AAWA)

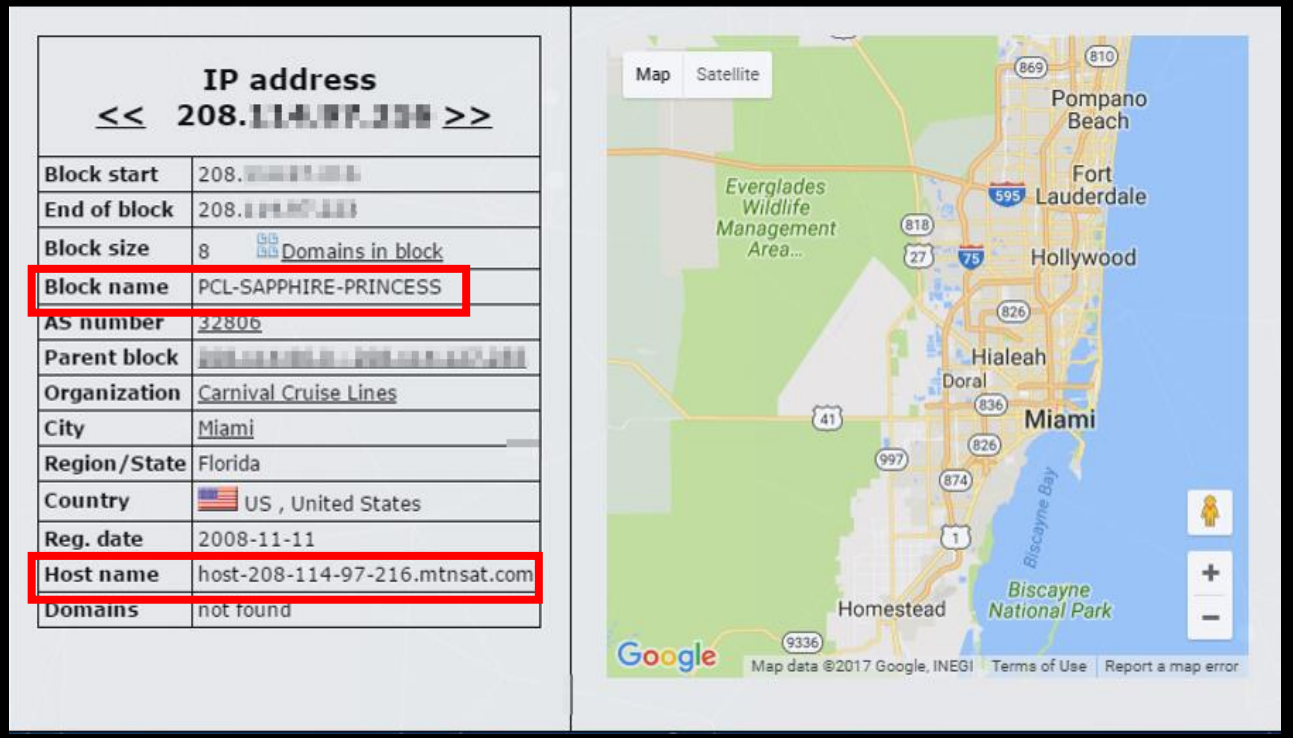


Vessel Digitization



Vessels Security Challenges

Vessels interconnection means more exposure to the world wide web



IP address << 208.[redacted] >>	
Block start	208.[redacted]
End of block	208.[redacted]
Block size	8 Domains in block
Block name	PCL-SAPPHIRE-PRINCESS
AS number	32806
Parent block	[redacted]
Organization	Carnival Cruise Lines
City	Miami
Region/State	Florida
Country	US , United States
Reg. date	2008-11-11
Host name	host-208-114-97-216.mtnsat.com
Domains	not found

Vessels Security Challenges

Data at Rest

Data in Transit

Intelligence

Crew Turnover

Deloitte.

Electronic Chart Display & Information System (ECDIS)

ECDIS Systems

- Geographic information systems
- International Maritime Organization compliant
- Alternative / compliant to paper nautical charts
- Can be interfaced with NavText and AIS
- July 2018 – Mandatory for all vessels in international voyages.

Attacking ECDIS Systems

- ECDIS systems are in essence desktop PCs
- With physical access a malicious person could use the USB slot to load incorrect/outdated maps, access the underlying operating system or spread malware/ransomware.

Attacking ECDIS Systems

- As with any other PC, ECDIS systems can be tampered with
- A number of these systems run with administrative rights and no password protection.

Deloitte.

Automatic Identification System (AIS)

AIS Systems

- Automatic tracking system for identifying and locating vessels
- 2002 – First mandate for vessels over 300GT to be equipped with a Class A type AIS transceiver.
- AIS information supplements marine radar, which continues to be the primary method of collision avoidance for water transport.
- Aid in accident investigation and in search and rescue operations.
- The information is also sent to providers such as Maritimetraffic.com, Vesselfinder.com or Aishub.net.
- Transmit in the Marine bands - Channel A 161.975 MHz (87B) & Channel B 162.025 MHz (88B)

AIS Systems Messages

AIS can send up to 27 types of messages

- Message 18 is sent between anywhere 30 seconds and 3 minutes to report the vessels position.
- Message 14 is a safety related broadcast used in emergencies.

Description	Value	Value Description
Vessel Name		
NMEA Sentence	!AIVDM,1,1,,A,>3a`Tn1@E	
Sentence Type	!AIVDM	
Fragments in this message	1	
Fragment No	1	
Sequential Message ID	(none)	
Radio Channel	A	
Payload	>3a`Tn1@E=B0tpiT	96 bits (16 6-bit words)
Fill bits * CRC check	0*52	
AIS Message		96 bits (12 8-bit words)
AIS Message Type	14	Safety Related Broadcast Message
Repeat Indicator	0	Repeatable
MMSI	244 983 000	Netherlands (Kingdom of the)
Spare	0	2 bits
Text	TEST ONLY	9 characters

AIS Systems Risks

- AIS communications do not employ authentication or integrity checks.
- Communication is made over RF
- Anyone with a cheap RF receiver can also “listen” to these messages. (Range dependent)

Maritime security - AIS ship data

At its79th session in December 2004, the Maritime Safety Committee (MSC) agreed that, in relation to the issue of freely available automatic information system (AIS)-generated ship data on the world-wide web, the publication on the world-wide web or elsewhere of AIS data transmitted by ships could be detrimental to the safety and security of ships and port facilities and was undermining the efforts of the Organization and its Member States to enhance the safety of navigation and security in the international maritime transport sector.

The Committee condemned the regrettable publication on the world-wide web, or elsewhere, of AIS data transmitted by ships and urged Member Governments, subject to the provisions of their national laws, to discourage those who make available AIS data to others for publication on the world-wide web, or elsewhere from doing so.

In addition, the Committee condemned those who irresponsibly publish AIS data transmitted by ships on the world-wide web, or elsewhere, particularly if they offer services to the shipping and port industries.

http://www.imo.org/en/ourwork/safety/navigation/pages/ais.aspx

AIS Attacks Landscape

Ship Hijacking

Hackers download the data of an existing ship, changing some of the parameters and submitting it to the AIS service.

AIS Spoofing

Hackers can send specially crafted messages that could mimic the location of an existing vessel, or even create a fake vessel and place it on its own virtual course.

Replay Attacks

Hackers capture and store AIS data and replay spoofed messages in specific timeframes

Arbitrary weather forecast

Hackers impersonate actual issuers of weather forecast such as the port authority and arbitrarily change the weather forecast delivered to ships.

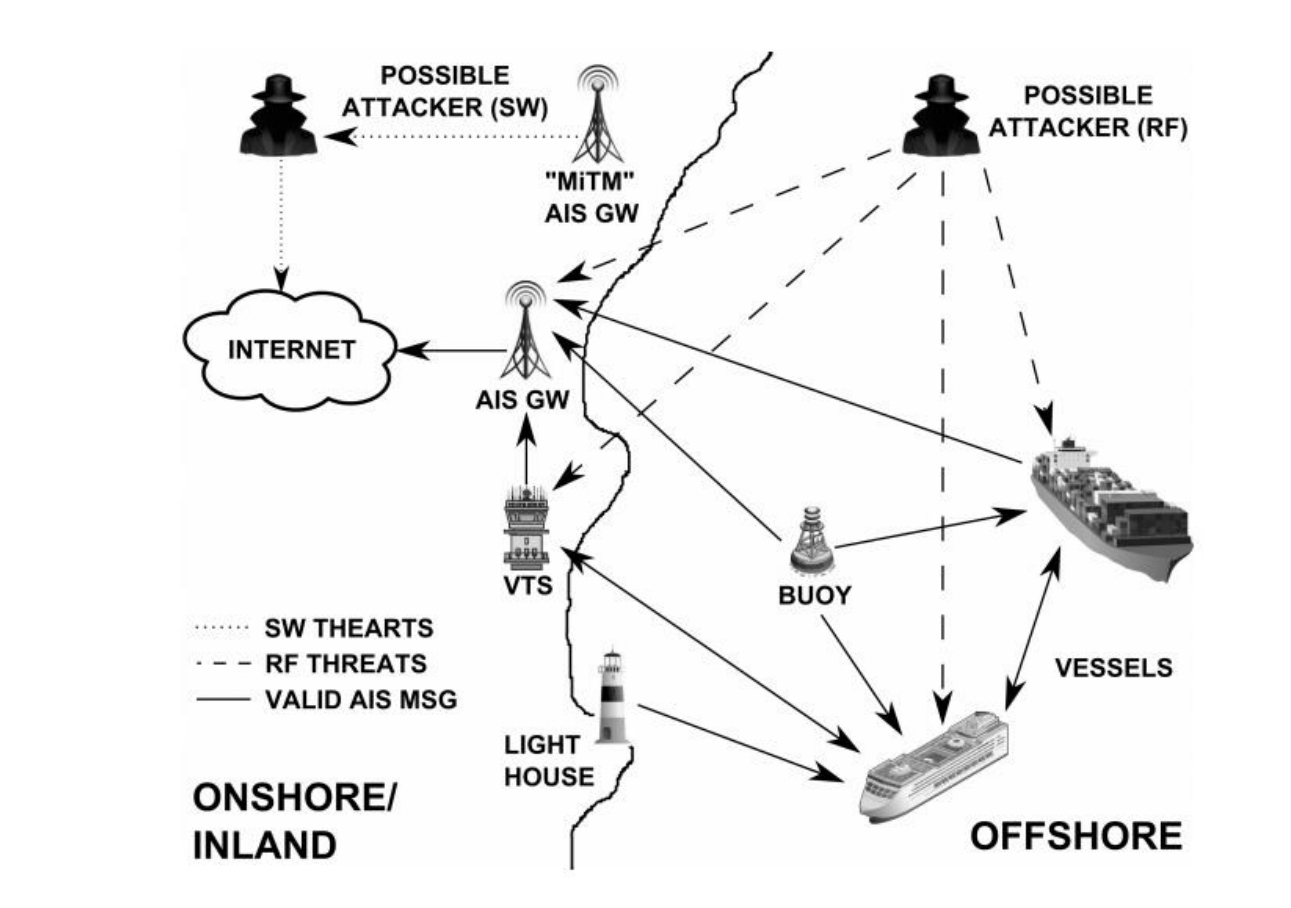
Man-in-the-water

Because of maritime laws and best practices, everyone needs to address this type of an alert.

Fake CPA

Hackers create a fake CPA (closest point of approach) alert.

AIS Systems Attacks



A Security Evaluation of AIS Automated Identification Systems
Marco Balduzzi, Alessandro Pasta, Kyle Wilhoit

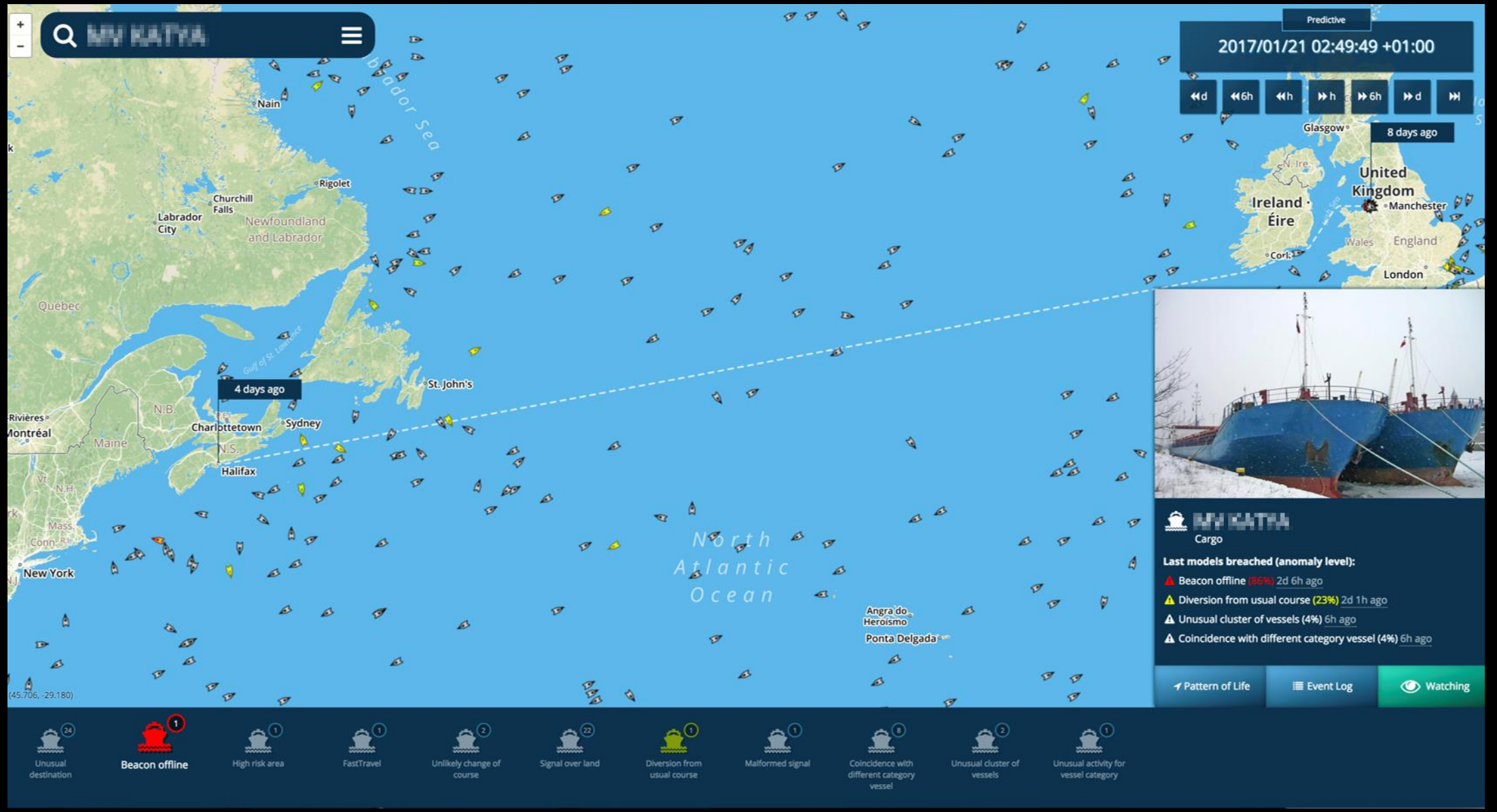
Even via RF the hackers have 4 attack vectors

- AIS Gateway
- Vessel Traffic Service
- Vessels
- Offshore

An exaggerated example?

1. 300 ton ships should not drive down the main street of a city

Deloitte’s Threat Analytics



AIS Systems Verified Attacks

- Modification of all ship details such as position, course, cargo, flagged country, speed, name & MMSI
- Creation of fake vessels e.g. having an vessel with nuclear cargo show up off the coast of the US
- Create and modify Aid to Navigations (AToN) entries, such as buoys and lighthouses.
- Research has been published in 2013 but since then there was not an improvement on the protocol
- ITU Radiocommunication Sector (ITU-R); the developers of the AIS standard and the protocol specification have acknowledged the problem

It’s not all bad…

Reliance on crew

- Sufficient and continuous training on Cyber Security
- Development of a Cyber Security Policy

Reliance on manual controls

- Crew
- Paper Charts
- Radar

Vessels must be treated as any other network

- Security Audits
- Penetration Testing
- Physical Security Assessments

Incident Response

- Development of Contingency Plans
- Stress Tests

Cyber Program

To be effective and well balanced, a cyber program must have three key characteristics: secure, vigilant, and resilient.

Being

SECURE

means having risk-prioritized controls to defend critical assets against known and emerging threats.

Being

VIGILANT

means having threat intelligence and situational awareness to anticipate and identify harmful behavior.

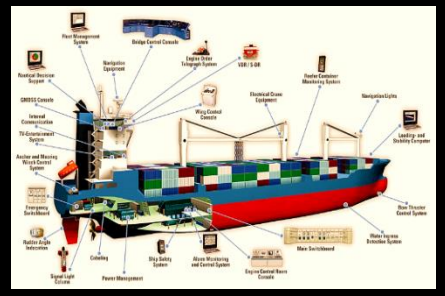
Being

RESILIENT

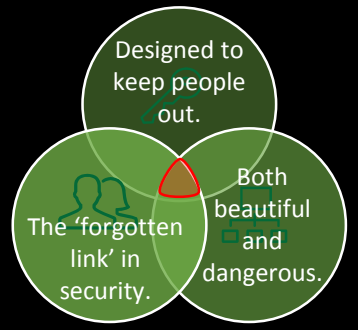
means being prepared and having the ability to recover from cyber incidents and minimize their impact.

Key Messages

Cyber risk is not an uncontrollable phenomenon



Maritime Industry is based on IT solutions with global interfaces to improve efficiency and international networking. Technical dimensions of shipping and of ships themselves are not depending on technology only for communication purposes. The **progress of information technologies will definitely proceed** and as a logical consequence, turn into complex risk-scenarios which currently seem to be difficult to be solved.



Balance people, processes and technology. Information security is not just about computer security. Computer security can carry the wrong assumption that as long as the infrastructure and systems are secure, the organization is also secure. You have to invest in all core elements of information security: physical, human and cyber.

Act as you have already been hacked. Breaches occur at all organizations – not because they are badly managed, but because hackers and cyber-criminals are getting smarter every day. Although it isn't possible for any organization to be 100 percent secure, it is entirely possible to use a mix of processes for prevention, detection and response to keep cyber-risk below a level set by the board and enable an organization to operate with less.

Four takeaway questions to reflect on through the lens of a secure, vigilant, and resilient approach to cybersecurity:

1 **Are we focused on the right things?**
Often asked, but difficult to accomplish. Understand how value is created in your organization, where your critical assets are, how they are vulnerable to key threats. Practice defense-in-depth.

2 **Do we have the right talent?**
Quality over quantity. There may not be enough talent to do everything in-house, so take a strategic approach to sourcing decisions. Are the security teams focused on the real business areas.

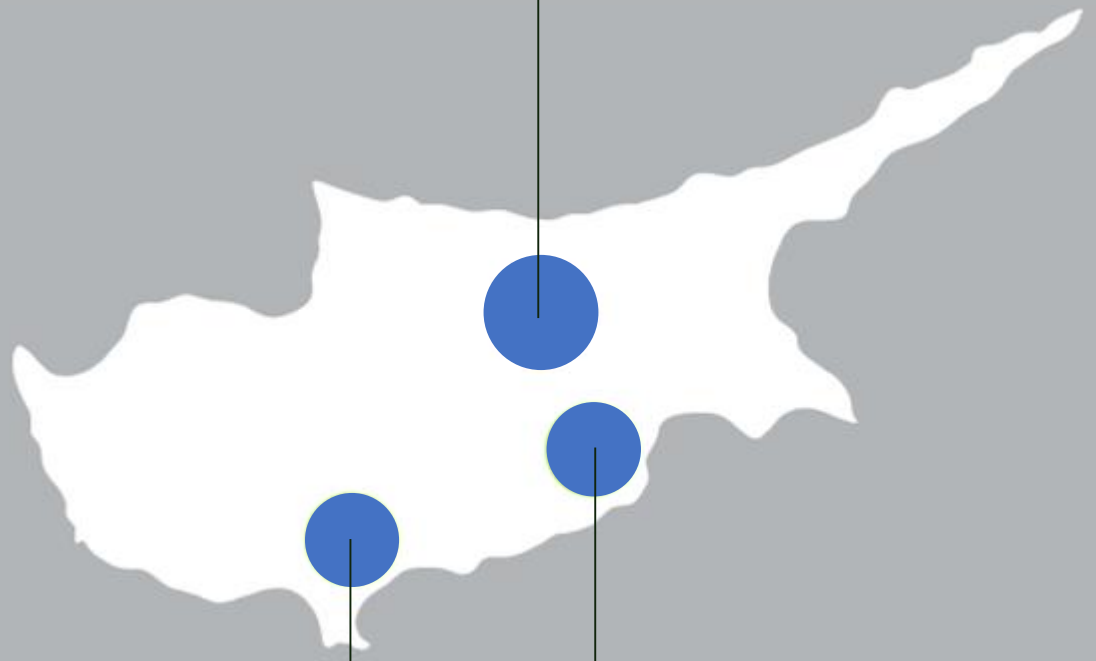
3 **Are we proactive or reactive?**
Retrofitting for security is very expensive. Build it upfront in your management processes, applications, and infrastructure.

4 **Are we adapting to change?**
Policy reviews, assessments, and rehearsals of crisis response processes should be regularized to establish a culture of perpetual adaptation to the threat and risk landscape.

Contact us

Nicosia
24 Spyrou Kyprianou Avenue
CY-1075 Nicosia, Cyprus
P.O.Box 21675
CY-1512 Nicosia, Cyprus

Tel.: +357 22360300
Fax: +357 22360400
E-mail: infonicosia@deloitte.com



Limassol
Maximos Plaza, Tower 1, 3rd floor
213 Arch. Makariou III Avenue
CY-3030 Limassol, Cyprus
P.O.Box 58466
CY-3734 Limassol, Cyprus

Tel.: +357 25868686
Fax: +357 25868600
E-mail: infolimassol@deloitte.com

Larnaca
Patroclos Tower, 4th floor
41-43 Spyrou Kyprianou Avenue
CY-6051 Larnaca, Cyprus
P.O.Box 40772
CY-6307 Larnaca, Cyprus

Tel.: +357 24819494
Fax: +357 24661222
E-mail: infolarnaca@deloitte.com

Deloitte.