Colombia mar 2023

VIII CONGRESO INTERNACIONAL DE DISEÑO E INGENIERIA NAVAL

¡MALWARE A BABOR!

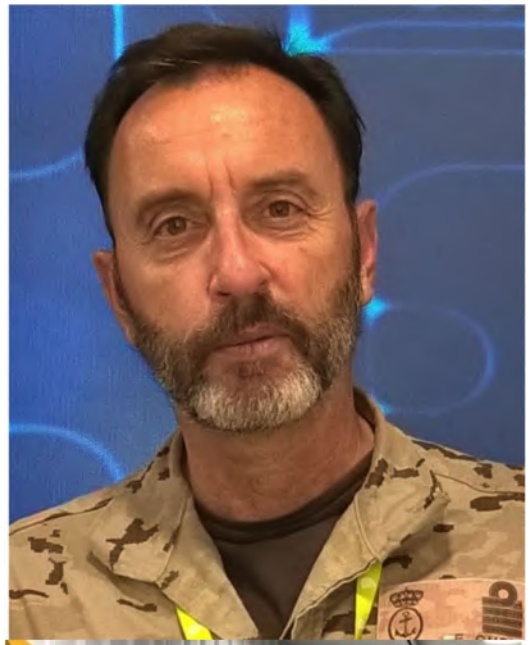
La Ciberseguridad en el ámbito marítimo

Enrique Cubeiro Cabello
Director de Ciberseguridad
GHENOVA

COLOMBIAMAR
Cartagena de Indias – 8 de marzo 2023

¿Quién soy?

Enrique Cubeiro

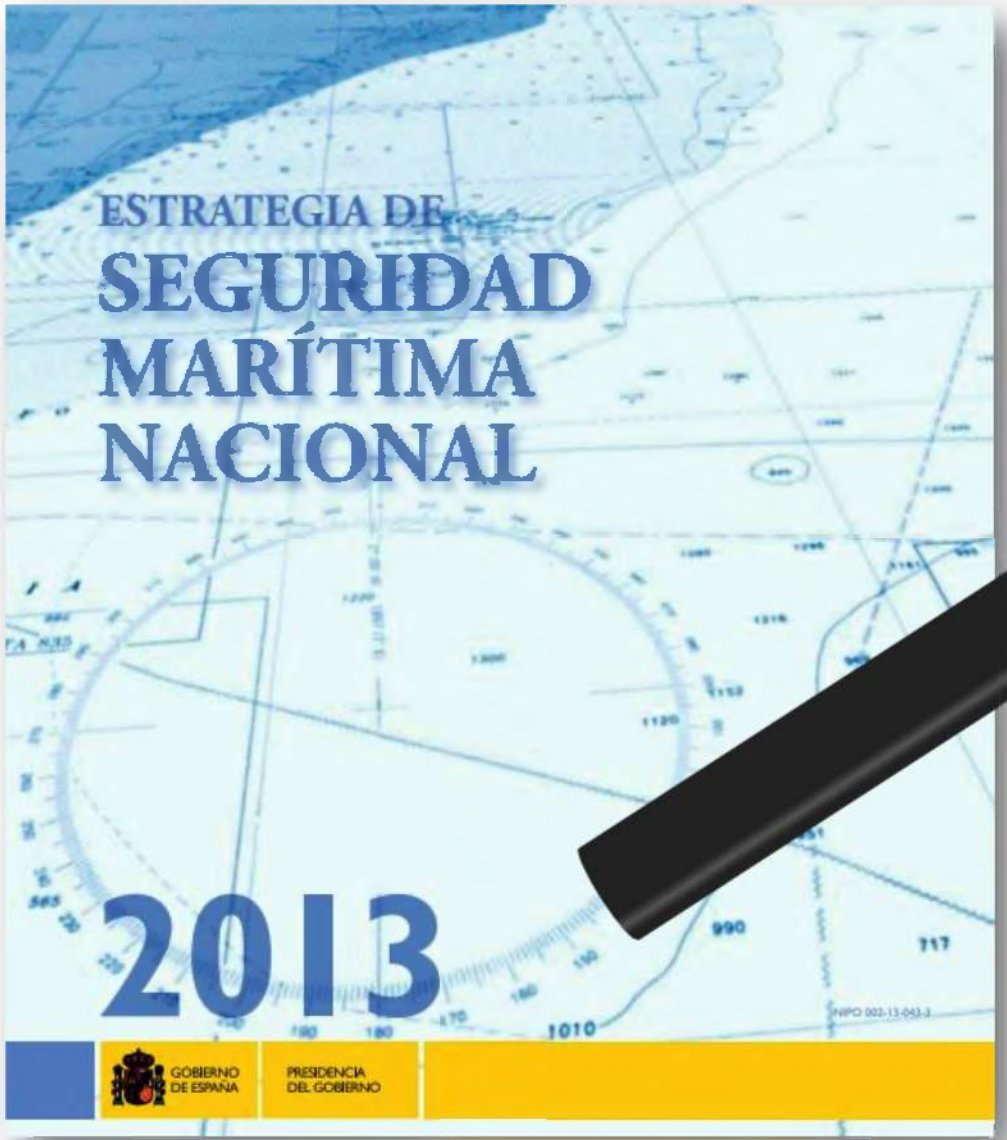


- Capitán de Navío (Reserva) de la Armada Española.
- Comandante buques “Bergantín” (1998-9), “Serviola” (2004-5) y “Patiño” (2012-13)
- Jefe de Operaciones MCCD (2013-2017).
- Jefe del Estado Mayor del MCCD (2017-2020).
- Jefe Área Ciberdefensa – JSSAT&CIBER - SDG Programas (DGAM) (2020-22).
- Director de Ciberseguridad de Ghenova (ENE2023 – continúa).
- Especialista en Comunicaciones.
- Diplomado en Estado Mayor Fuerzas Armadas.
- Master Ciberdefensa Univ. Alcalá de Henares (Madrid).
- Cursos diversos sobre Cyberdefence en CCD CoE (Tallin, Estonia).
- Presidente GT desarrollo L.A. Potenciación Ciberseguridad Ámbito Marítimo (2014).
- Integrante del grupo expertos elaboración ENCS 2019.
- Representante MDEF en GGTT desarrollo planes acción ENCS 2013 y 2019.
- Presidente GT elaboración Guía buenas prácticas ciber buques y puertos (2020)

Índice

Índice

Introducción



LÍNEA DE ACCIÓN 5

Mejora de la ciberseguridad en el ámbito marítimo

El carácter esencial de las TIC en el ámbito marítimo r… aciones concretas en el marco de la ciberseguridad de… evalua… …ora de los estándares de seguridad marítima nacio… …timo, así

…ario fomentar un enfoque integral de la… …an actuaciones …cción, explotación, …gos y amenazas cibernéticos… …s en el espacio marí… …ión de todos los…

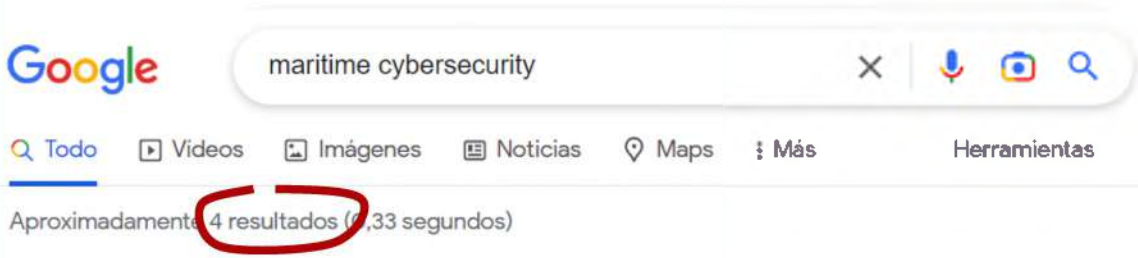
Se añadi… …las Redes de Telecomunicaciones y a los Sistemas de Información… así como en el desarrollo y aplicación de tecnologías específicas, para reforzar las estructuras de seguridad, la capacidad de vigilancia, de prevención y de respuesta de dichos sistemas.

El intercambio de información, la cooperación y colaboración público-privada también en el entorno internacional, así como el desarrollo de estándares y mejores prácticas en ciberseguridad en el ámbito marítimo son también actuaciones de carácter prioritario.

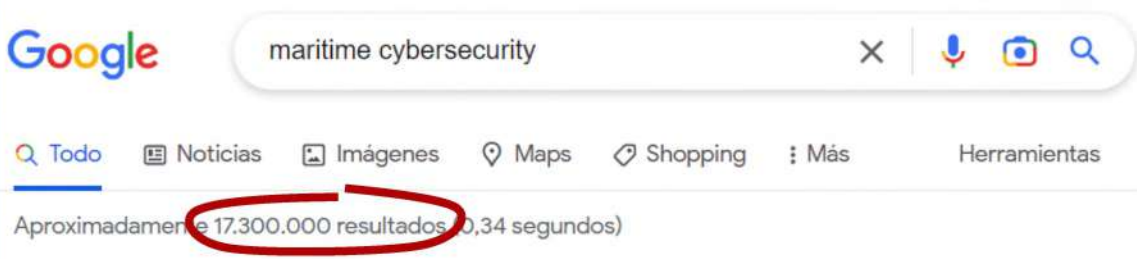
Igualmente es necesario crear un marco de conocimientos específicos sobre la materia dirigido a los profesionales del ámbito marítimo, así como actuaciones de concienciación y sensibilización en este campo específico.

Introducción

2013



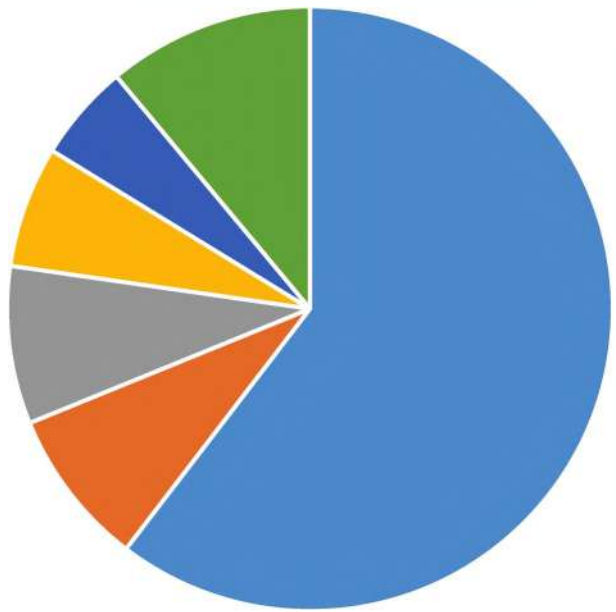
2023



Introducción

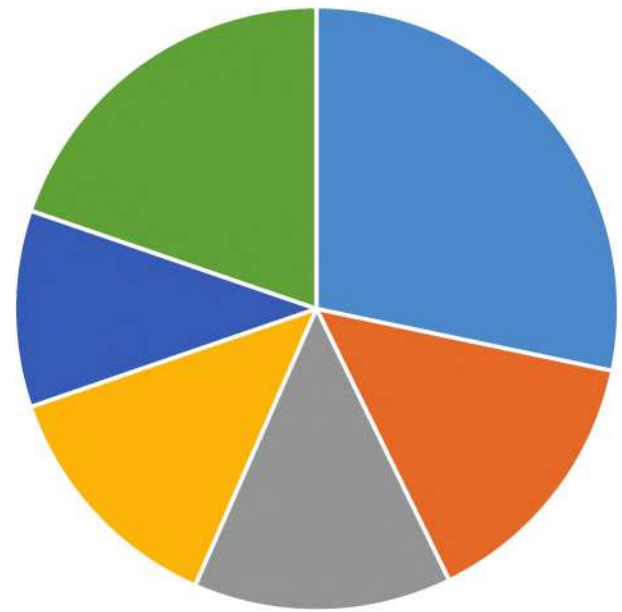
2013

CIBERATAQUES POR SECTORES



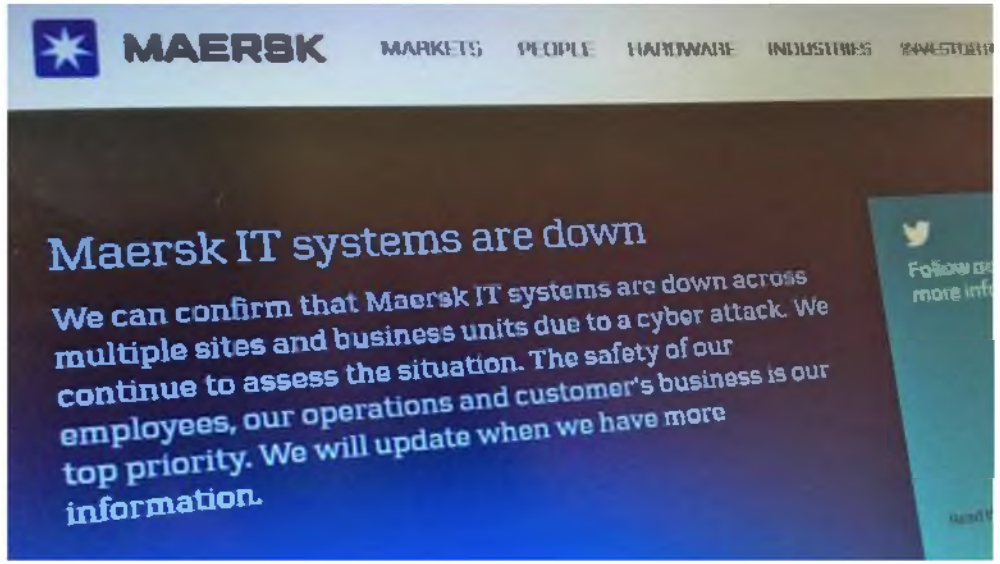
2023

CIBERATAQUES POR SECTORES



Introducción

Ciberataque NotPetya (ramsonware), julio 2017



Coste para la compañía Maersk: aprox. 300 M $

Introducción

Las ciberamenazas:

- Persiguen el dinero / el daño.
- Atacan a la información / los datos.
- Buscan sistemas mal protegidos.
- Explotan las vulnerabilidades de las tecnologías.
- Procuran la máxima rentabilidad del esfuerzo.
- Explotan las vulnerabilidades del entorno.

Ámbito marítimo:

- Mucho dinero / Mucho que dañar.
- Mucha información (operativa, logística, meteorológica, ...)
- Muchos sistemas heredados / obsoletos.
- Interconexiones numerosas
- Convergencia sistemas IT/OT.
- Nuevas tecnologías (fe ciega).
- Globalización.
- Escasa concienciación.
- Complejidad idiomática.
- Amplitud de las relaciones (agencias, clientes, armadores, ...).

Introducción

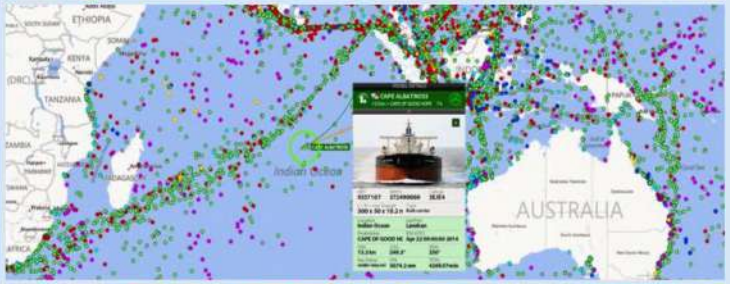
Introducción

Sistemas específicos del ámbito marítimo:

- De barcos.
- De puertos.
- De apoyo/auxilio a la navegación.
- De navieras (?).





Introducción

Galera (siglo I)

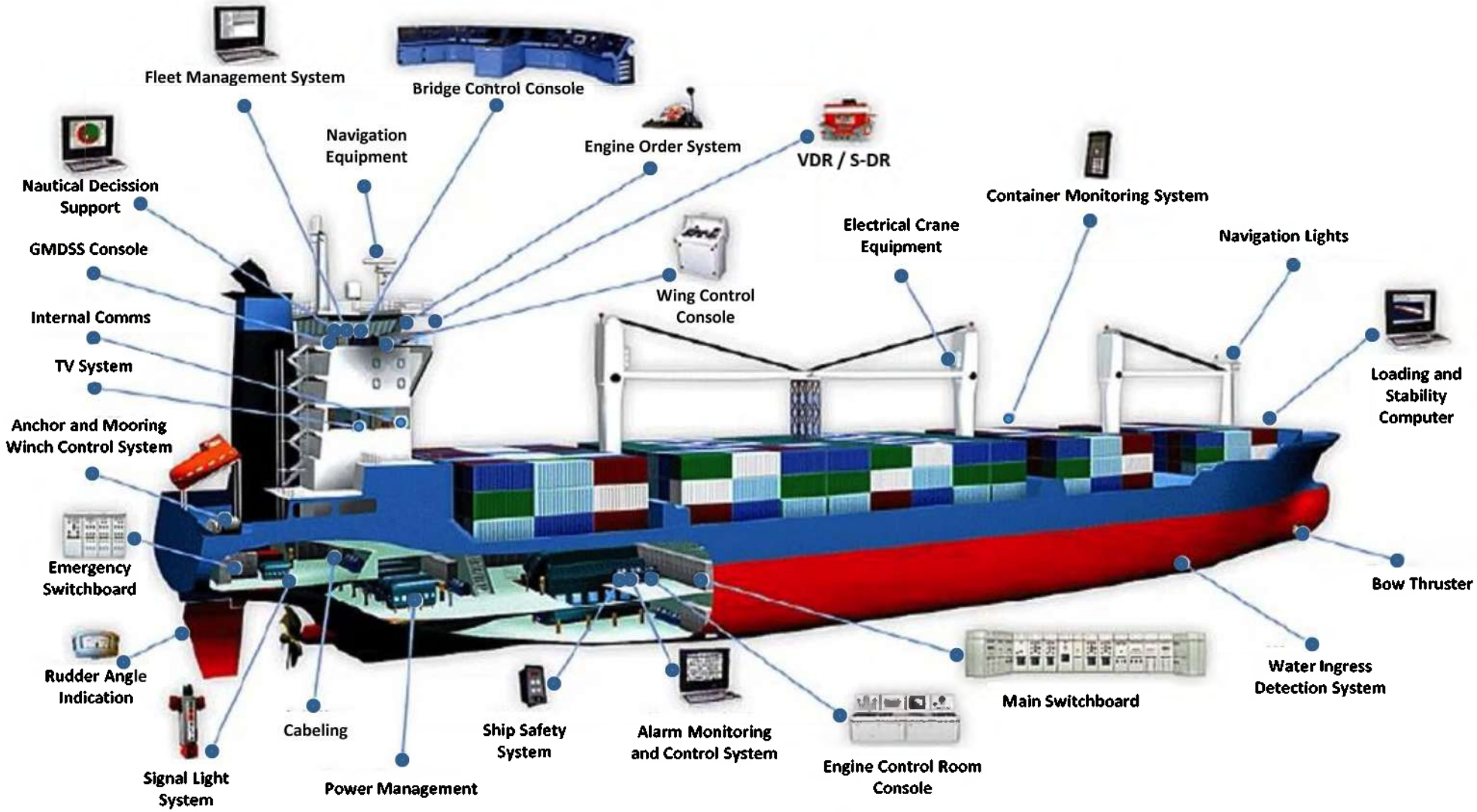
Carabela (siglo XV)

Destructor ARC *"Antioquia" (1943-1973)*

Fragata "Baleares" (1973-2005)

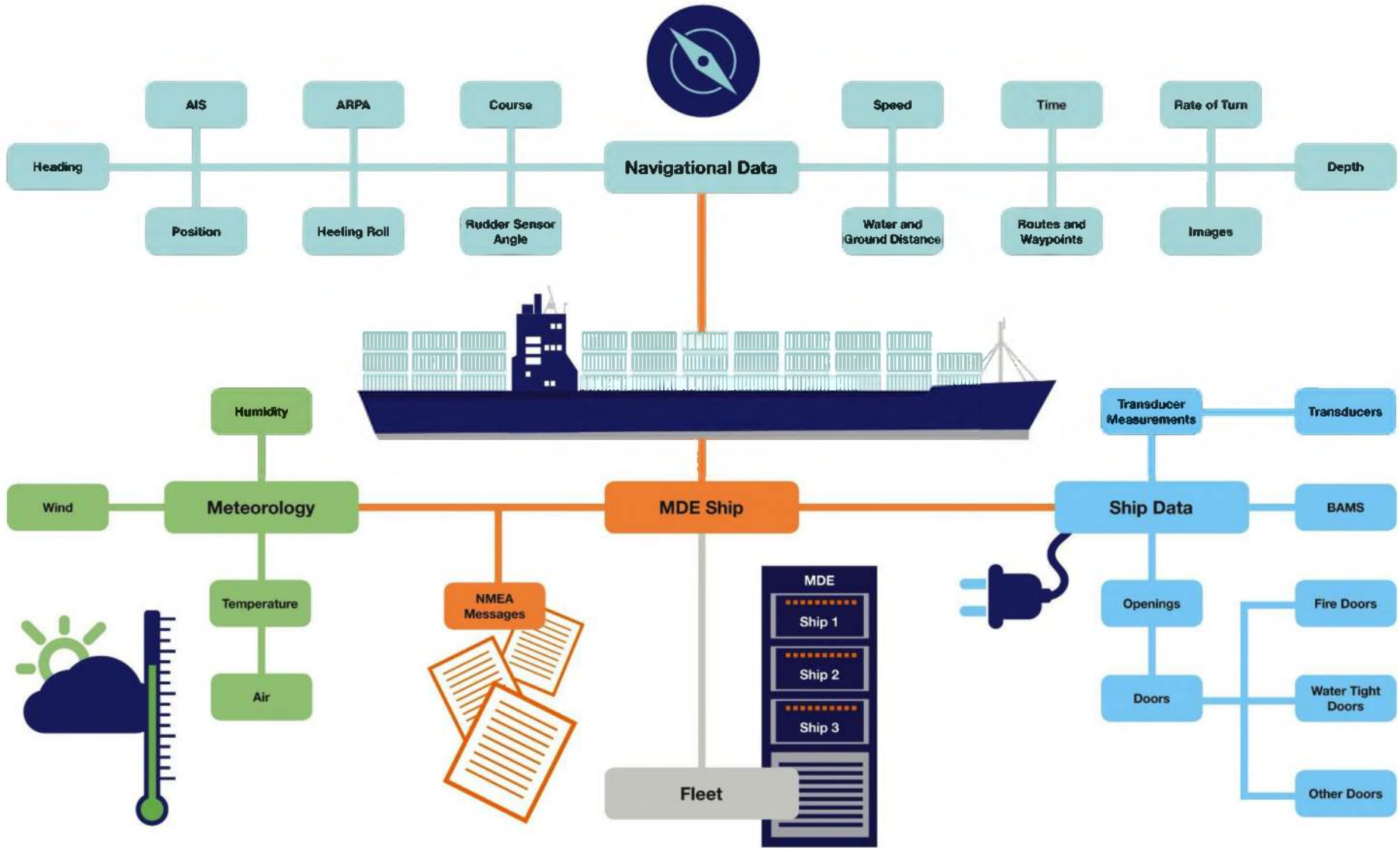
Introducción

Sistemas a bordo (mercantes)



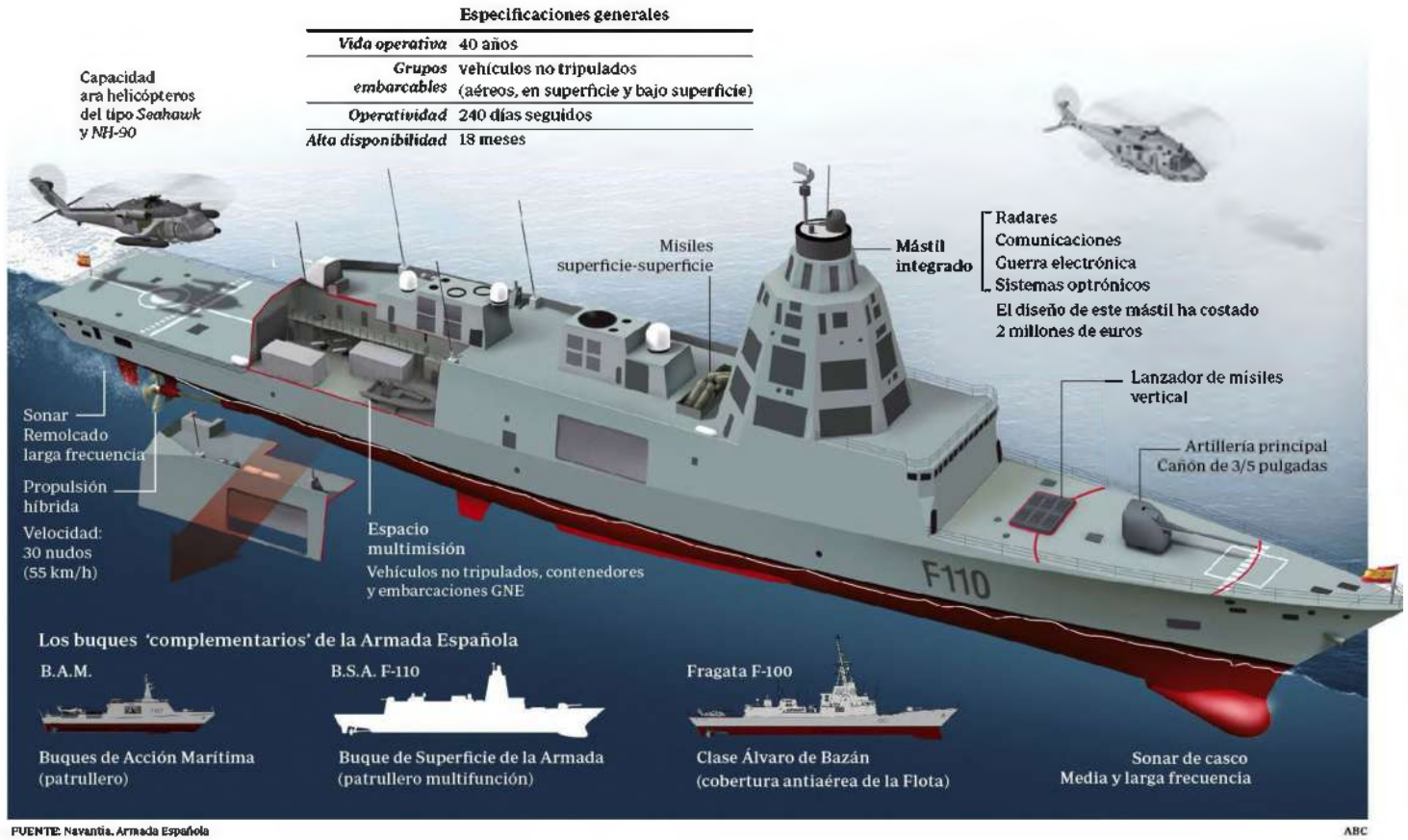
Introducción

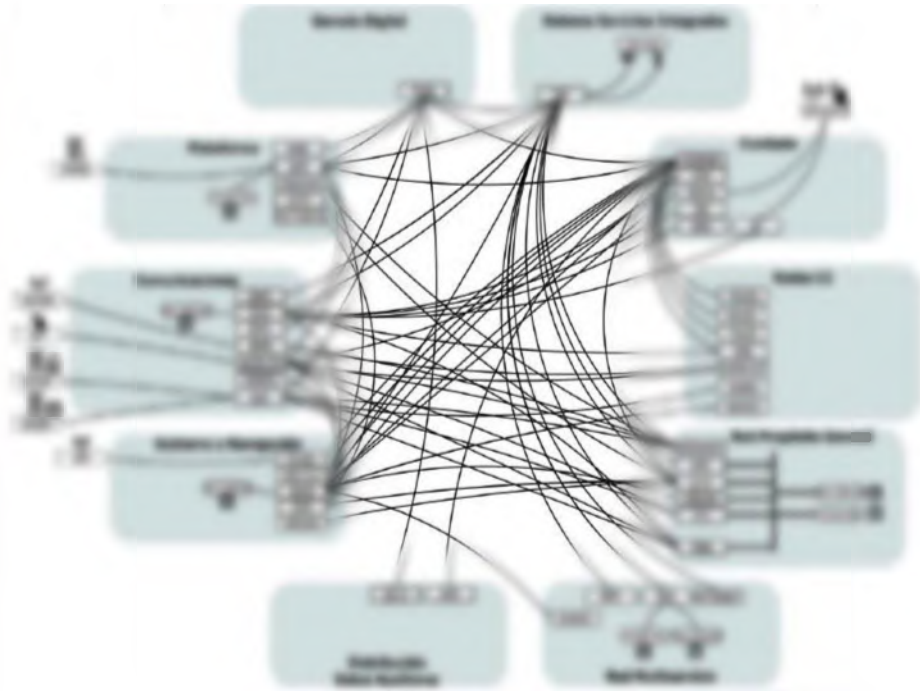
Sistemas a bordo (mercantes)



Introducción

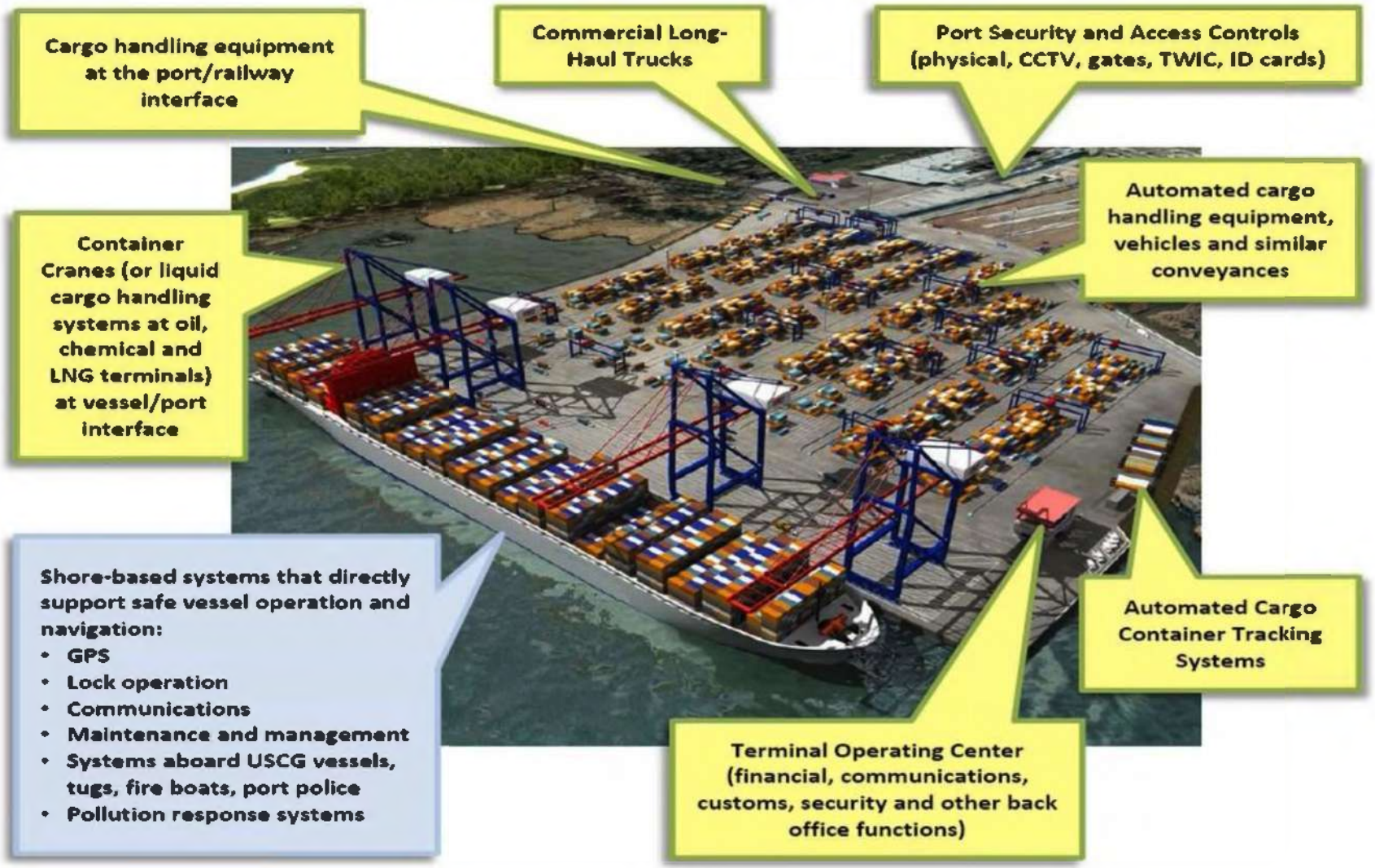
Sistemas a bordo (buques de guerra)





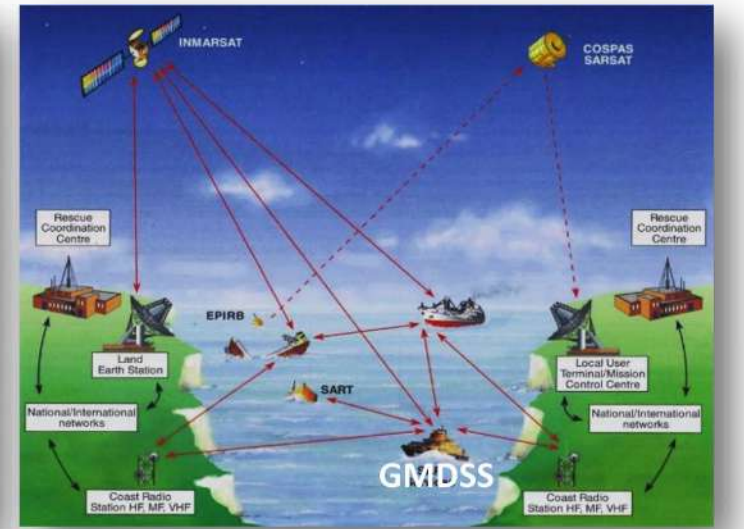
Introducción

Sistemas portuarios



Introducción

Sist. de posicionamiento, ayuda a la navegación, oceanográficos y meteorológicos



Introducción

Posibles objetivos

Comunes a cualquier ámbito/sector

- Sistemas operativos (Microsoft, Linux, MacOS, Symbian, Android, …).
- Enterprise Resource Planning (ERP) Systems (financieros, logísticos, de pago, aduaneros, …).
- Aplicaciones software empresarial (financieras, logísticas, operaciones comerciales, RRHH, …).
- Sistemas de seguridad: CCTV, control de acceso, …
- Dispositivos y plataformas de movilidad (EFB).
- Sistemas de comunicaciones (incluido e-mail).
- Empleados / usuarios.

Propios del Sector marítimo

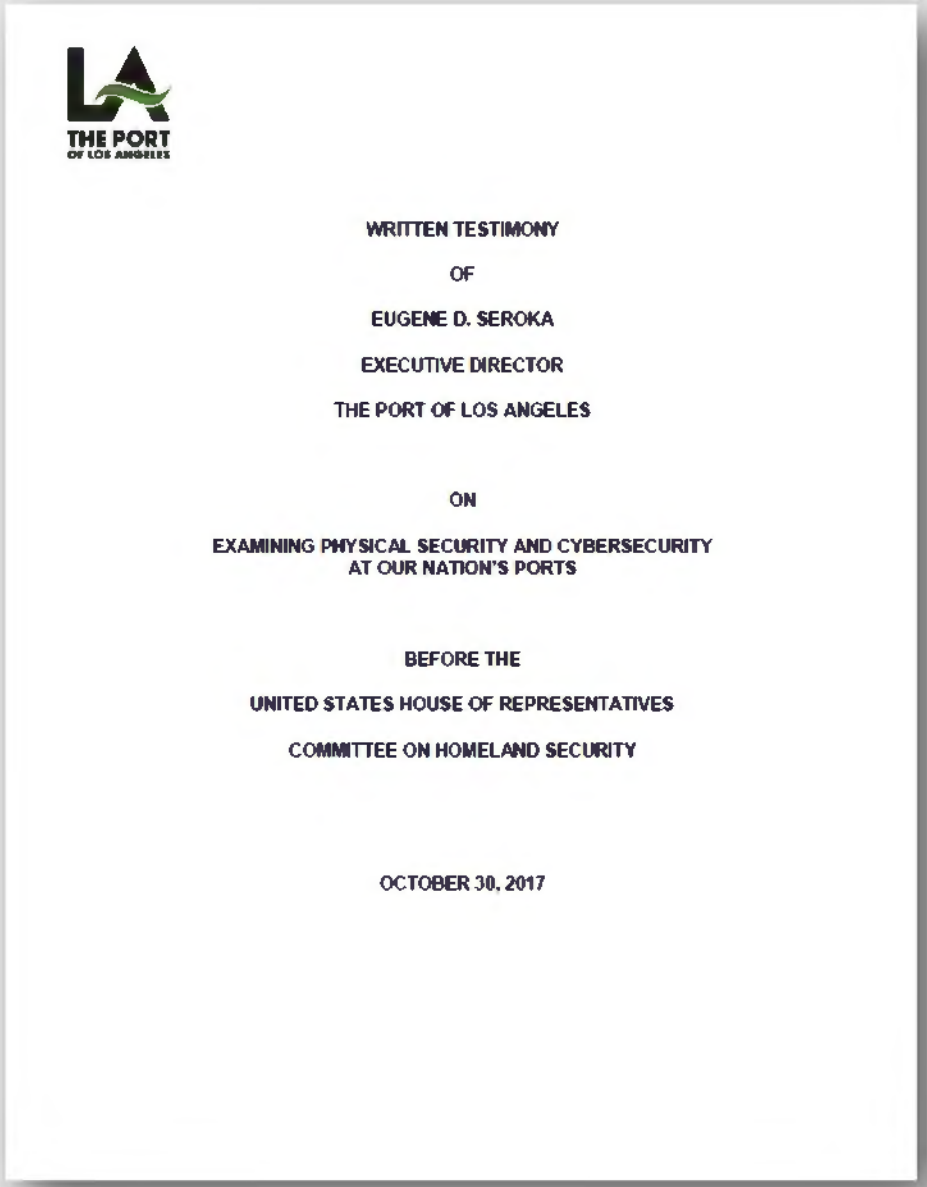
- Equipos SCADA, sistemas de control industrial (ICS) de buques y puertos.
- Sistemas integrados de control de plataforma (SICP).
- Sistemas de gestión de carga / terminal.
- Sistemas de ayuda a la navegación: RADAR, AIS, VTS / VTMS, ECDIS, VDR, etc.
- Sistemas de posicionamiento: GPS, Galileo, BeiDou, NAVSTAR, GLONASS, …

Militares

- Sistemas de Mando y Control Militar
- Sistemas de combate.
- Sistemas de armas.

Índice

La amenaza



THE PORT OF LOS ANGELES

WRITTEN TESTIMONY

OF

EUGENE D. SEROKA

EXECUTIVE DIRECTOR

THE PORT OF LOS ANGELES

ON

EXAMINING PHYSICAL SECURITY AND CYBERSECURITY AT OUR NATION'S PORTS

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

OCTOBER 30, 2017

The Security Operations Center plays an invaluable role for the Port (of Los Angeles) and is managing an unprecedented level of attacks: over 20-million cyber intrusion attempts per month, literally ***seven-to-eight attacks every second*** *on average.*

The Port is seeing a growing volume and variety of malicious cyberattacks ranging from denial-of-service attacks, more standard data breaches, botnet and malware attacks along with possible insider threats.

(Octubre 2017)

La amenaza

Actores	Acciones	Motivaciones
Hackers	Robo de credenciales Penetración en el sistema	Muy diversas
Insiders	Robo de información Sabotaje	Venganza Ideológica Económica
Crimen organizado	Robo de información *Ransomware* *CaaS*	Económica
Actores comerciales	Robo de información Ciberespionaje	Posicionamiento empresarial
Hacktivistas	*Web defacement* Robo y exposición información Sabotaje / Ataques DDoS	Ideológica Política
Ciberterroristas	Sabotaje Ciberataque a ICs	Ideológica Política
Actores-Estado	Ciberespionaje Sabotaje / Ciberguerra Ciberataque a ICs	Poder del Estado

La amenaza

Posibles técnicas y vectores de entrada

- **Acciones precursoras:**
  - Correo electrónico (spoofing/phishing).
  - Dispositivo USB infectado.
  - Suplantación de punto de acceso WiFi.
  - Inyección SQL.
  - Acceso no autorizado a sistema / robo o ruptura de contraseña.
    - Keylogger
    - Baiting.
    - Ingeniería social.
    - Ataque de fuerza bruta.
    - Ataque de diccionario.
    - Shoulder-surfing.
    - Trashing.
    - Insider.
- **Acciones sobre el objetivo:**
  - Ataque DDoS contra activos expuestos a Internet.
  - Defacement (alteración del aspecto) de activos expuestos a Internet.
  - Robo de información / datos.
  - Alteración o borrado de información / datos con fines de sabotaje.
  - Cifrado de información/datos a cambio de rescate (ransomware).
  - Acceso remoto a dispositivos.
  - Control remoto de elementos.

La amenaza

Sistemas de a bordo desde la perspectiva de un hacker

Phishing email
DDoS
Ataque de diccionario
Troyano
Ingeniería social
Malware
Fuerza bruta
Spoofing
Rogue WiFi
Exploit kit
USB infectado
Ransomware

Seguridad de red
- Firewalls
- Segmentación
- Dispositivos seg. perimetral

Comunicaciones
- Email
- Internet vía satélite
- Buque – Tierra
- Buque – Buque
- Radio/PMR
- VoIP

Seguridad física
- Local de servidores
- Locales de máquinas
- Infraestructura de red
- Control de accesos
- Puente

Actualizaciones y Administración remota

Red del buque
- Email
- Carga
- Antivirus
- Mantenimiento programado
- Entradas USB
- Nómina

Red dotación
- WiFi
- BYOD
- Email
- Navegación web
- Entretenimiento

Navegación
- Radar
- GPS
- ECDIS/Cartografía
- Giroscópica
- Cartografía
- Sistemas meteorológicos

Carga y estabilidad
- Software de gestión de carga
- Monit. de esfuerzos de casco
- Sistema de lastre
- Mensajería UN/EDIFACT

La amenaza

Posibles escenarios

- Manipulación sistemas buque/puerto para provocar accidente o situación de riesgo (varada, colisión, derrame, explosión, incendio, ...).
  - Sistemas del puente (posicionamiento, gobierno, control, comunicaciones).
  - SICP / Control de la propulsión / Control de la planta eléctrica.
  - Sistemas de armas / combate.
  - Sensores de emergencia.
- Manipulación de la cartografía digital.
- Manipulación de sistemas de posicionamiento (por ejemplo, GPS).
- Manipulación de sistemas de identificación (por ejemplo, AIS).
- Manipulación de sistemas ICS/SCADA para movimientos de carga.
- Ataque ransomware a sistema/aplicación que paralice operativa portuaria.
- Ataque contra la disponibilidad de bases de datos o aplicaciones logísticas.
- Ataque contra la integridad de bases de datos o aplicaciones logísticas.
- Robo de información financiera.
- Robo de información de clientes.
- Bloqueo de sistemas web para gestión portuaria.
- Bloqueo del correo electrónico.
- Alteración de sensores de información meteo (altura de olas, vientos, etc.)

Índice

Capitán, tenemos un problema

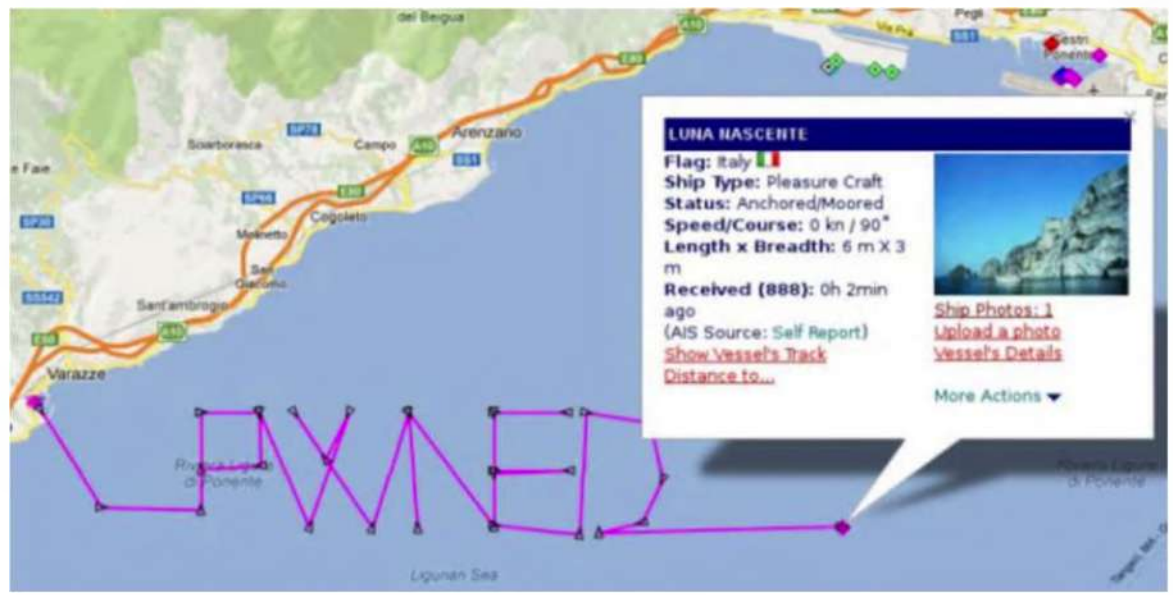
OCT
2013

OCEANEERING®

Hackers Figured Out How to Hijack Shipping Vessel Tracking Systems

Adam Clark Estes
10/18/13 10:20am • Filed to CYBERSECURITY

38 Save



Earlier this month, researchers at a "hacker's conference" in Kuala Lumpur were able to demonstrate what on the surface appeared to be some serious vulnerabilities to the Automatic Identification System (AIS). During this session, researchers were able to make vessels "disappear", spoof vessel transmissions, and introduce new vessel tracks on an AIS-based display.

Capitán, tenemos un problema

MAR
2015

Hacking Ships: Maritime Shipping Industry at Risk

March 31, 2015 By Pierluigi Paganini

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

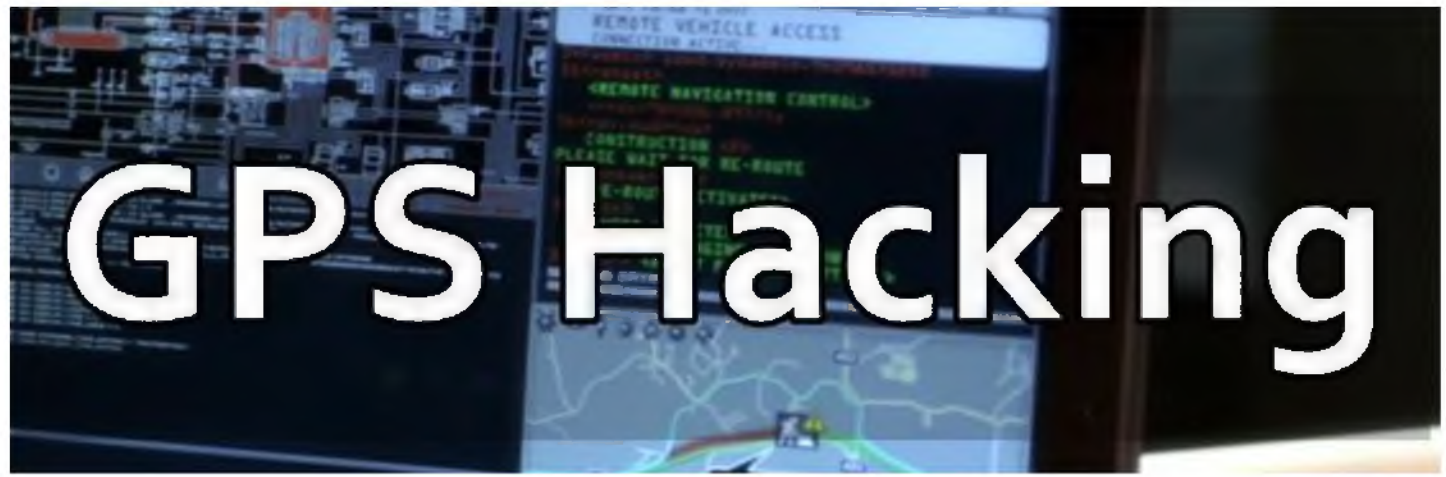
Hackers target Cyber Attack on Ships: Maritime Shipping Industry at Risk

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

Capitán, tenemos un problema

NOV
2016

TECHWORM



GPS spoofing and dangers of GPS data hacking

By **vijay** - November 29, 2016 156 0

Hacking Global Positioning System with GPS 'Spoofing' Can Lead To Fatalities

Capitán, tenemos un problema

JUN
2017

NL#TIMES

Rotterdam Port, TNT hit in new ransomware attack

WEDNESDAY, 28 JUNE 2017 - 08:29

Countless computers across the world were infected with ransomware in a new global cyber attack. In the Netherlands the malware hit the APM container terminal in the port of Rotterdam, pharmaceutical MSD and package carrier TNT. There is no sense in paying the ransom, cyber security experts warn, broadcaster NOS reports.

Capitán, tenemos un problema

AGO
2017

threatpost

Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack

Author:
Michael Mimoso

August 16, 2017 / 1:33 pm

A.P. Moller-Maersk, the world's largest container ship and supply vessel company, said Tuesday that it would incur hundreds of millions in U.S. dollar losses due to the NotPetya wiper malware attacks of late June.

Capitán, tenemos un problema

AGO
2017

THE STRAITS TIMES

WORLD

US warship collisions raise cyber attack fears

The USS John S McCain as seen in Changi Naval Base on Aug 22, 2017. ST PHOTO: KEVIN LIM

SINGAPORE (AFP) - A spate of incidents involving United States warships in Asia, including a deadly collision this week off the Singapore coast, has forced the US Navy to consider whether cyber attackers might be to blame.

Capitán, tenemos un problema

OCT
2017

BLEEPINGCOMPUTER

To Nobody's Surprise, Ships Are Just as Easy to Hack as Anything Else

By Catalin Cimpanu

October 14, 2017 03:00 AM 0

Modern-day ships aren't that hard to hack according to Ken Munro, a security researcher at Pen Test Partners, a UK cyber-security company.

Capitán, tenemos un problema

RESILIENT NAVIGATION and TIMING FOUNDATION

Hackers took ‘full control’ of container ship’s navigation systems for 10 hours

Tanya Blake, editor, Safety at Sea | 22 November 2017

NOV
2017

In February 2017 hackers reportedly took control of the navigation systems of a German-owned 8,250 teu container vessel en route from Cyprus to Djibouti for 10 hours. “Suddenly the captain could not manoeuvre,” an industry source who did not wish to be identified told *Fairplay* sister title *Safety At Sea* (*SAS*). “The IT system of the vessel was completely hacked.”

Capitán, tenemos un problema

DIC
2017

El ciberataque a Maersk 6 meses después

*kapil patel **25** de diciembre 2017*

El ciberataque de junio de 2017 a Maersk afectó a las terminales de envío en todo el mundo e incluso provocó el cierre del puerto de Los Ángeles, una de las terminales de carga más grandes del mundo, durante unos días.

Las operaciones se interrumpieron, los puertos tuvieron que cerrarse y Maersk tuvo que volver a realizar negocios en papel solo para que las mercancías se trasladaran de los barcos a la costa nuevamente. El ataque le costó al gigante naviero danés entre 200 y 300 millones de dólares y ha cambiado definitivamente la forma en que la industria del transporte marítimo ve la ciberseguridad.

Capitán, tenemos un problema

ENE
2018

BLEEPINGCOMPUTER

Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack

By Catalin Cimpanu January 25, 2018 06:45 AM 2

The world's largest container shipping company —A.P. Møller-Maersk— said it recovered from the NotPetya ransomware incident by reinstalling over 4,000 servers, 45,000 PCs, and 2500 applications over the course of ten days in late June and early July 2017.

Capitán, tenemos un problema

FEB
2018

News Deeply
OCEANS DEEPLY

Hacked at Sea: Concerns Grow Over Lax Cybersecurity for Ships, Ports

As hacking risks grow and maritime operations become more digitally connected, experts in industry and government have long said no one is prepared. This summer was a wake-up call.

WRITTEN BY	PUBLISHED ON	READ TIME
Jessica Leber	Feb. 5, 2018	Approx. 7 minutes

A container ship arriving at Port Newark in New Jersey. James Levine Corbis via Getty Images

Capitán, tenemos un problema

ABR
2018

techworld
FROM IDG

Can you hack a ship? Global maritime industry ripe for hacking

Security researchers have for years been warning the maritime industry that it is low hanging fruit as incredibly high-value cargo is fitted to ships with legacy (at best) systems, bad awareness, poor processes, and seaports that can suffer from the same problems.

By Tamlin Magee | Apr 03, 2018

The maritime shipping industry is the main conduit for global trade, with more than 80 percent by volume transported from region to region by ships, and 10.3 billion tons in total moving between seaports around the world globally in 2016. Despite this, incident after incident has demonstrated just how much the trillion dollar industry is open to cyber attack.

Security researchers have for years been warning the maritime industry that it is low hanging fruit as incredibly high-value cargo is transported on ships with legacy systems, combined with poor processes and awareness, while the seaports they dock in often suffer from the same problems.

Capitán, tenemos un problema

JUN
2018

BBC NEWS

Technology

Ship hack ‘risks chaos in English Channel

By Leo Kelion
Technology desk editor

7 June 2018 Share

The English Channel is the busiest shipping route in the world

A commonly used ship-tracking technology can be hacked to spoof the size and location of boats in order to trigger other vessels' collision alarms, a researcher has discovered.

Ken Munro has suggested that the vulnerability could be exploited to block the English Channel.

Capitán, tenemos un problema

JUL
2018

≡ EL PAÍS

TECNOLOGÍA

50.000 barcos en el mundo son vulnerables a los ciberataques

Varios problemas hacen que al sector marítimo le resulte especialmente difícil abordar la ciberseguridad

KITH MARTIN Y RORY HOPCRAFT

19 JUL 2018 · 09:56 CEST

Capitán, tenemos un problema

JUL
2018

WORLD MARITIME NEWS

COSCO Shipping Lines Falls Victim to Cyber Attack

Image Courtesy: Kees Torn

COSCO Shipping Lines confirmed that it has been hit by a cyber attack impacting its internet connection within its offices in America.

As such, local email and network telephone were not working properly and the company decided to shut down the connections with other regions for further investigation.

Based on the information released so far, the incident that took place on Tuesday, July 24, was described as a ransomware attack.

The Chinese shipping and logistics company said that its vessels were not impacted and that its main business operation systems were performing stably. However, COSCO's terminal at the Port of Long Beach was affected.

Capitán, tenemos un problema

SEP
2018

LA VANGUARDIA | Barcelona

Al Minuto Internacional Política Opinión Vida Deportes Economía Local Gente Cultura Sucesos Temas

AFECTA A VARIOS SERVIDORES

El Puerto de Barcelona sufre un ciberataque que podría retrasar la entrega de mercancías

• Los puertos y los buques estánconsideradas como las nuevas infraestructuras críticas en ciberseguridad, por los daños potenciales que podría causar un ataque a gran escala

REDACCIÓN
20/09/2018 13:17

Actualizado a
20/09/2018 15:13

Una imagen del Puerto de Barcelona (Getty)

Capitán, tenemos un problema

SEP
2018

ZDNet

Port of San Diego suffers cyber-attack, second port in a week after Barcelona

Cyber-attacks have now been reported at three ports in the last two months

By Catalin Cimpanu for Zero Day | September 27, 2018 -- 16:24 GMT (17:24 BST) | Topic: Security

Two major international ports fell victim to cyber-attacks within the span of a week, putting the shipping industry on alert for a possible threat actor targeting the entire sector.

The first to fall was the Port of Barcelona, Spain, on September 20, last week. The second attack was reported yesterday, September 25, by the Port of San Diego, in the United States.

Capitán, tenemos un problema

JUL
2019

naked security
by SOPHOS

Cyberattack lands ship in hot water

11 JUL 2019 1
Malware, Security threats

On Monday 8 July 2019 the Coast Guard issued a Marine Safety Alert reporting a successful malware attack on a vessel back in February. The crew avoided losing complete control of the ship, but it should be a wake-up call. The report explained the findings of the cybersecurity team that investigated the incident:

The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted.

Capitán, tenemos un problema

MAY
2020

ALJAZEERA

Israel cyberattack caused ‘total disarray’ at Iran port

Security officials say strike on Shahid Rajaee terminal was ‘tit-for-tat’ after alleged hack in Israel: Washington Post.

19 May 2020

Israel has been accused of launching a major cyberattack on an Iranian port that caused transport chaos for days after crashing the facility’s computer system, a news report said on Tuesday. Iran’s Shahid Rajaee terminal, near the Iranian coastal city of Bandar Abbas on the Strait of Hormuz, was suddenly hit by hackers, crippling the port on May 9, the Washington Post reported.

An Iranian inspector walks past shipping containers at Shahid Rajaee port, 20km west of Bandar Abbas city [File: Behrouz Mehri/AFP]

Capitán, tenemos un problema

OCT
2020

EuropaSur

La naviera CMA CGM se recupera de un ciberataque que no afecta a los puertos

A. R. ALGECIRAS, 02 OCTUBRE, 2020 - 10:58H

La naviera **CMA CGM**, tercera del mundo por volumen de negocio, se recupera progresivamente de un **ciberataque** sufrido a mediados de esta semana y que ha afectado al **sistema de comunicaciones** de la compañía. Según la firma, sus **operaciones en los puertos** no se han visto afectadas.