

# Cyber Security And Future-Proofing Your IT Infrastructure

Emmanouil CHRISTOFIS  
Cyber Defence Capabilities specialist

## Consumer & Home



## Smart Infrastructure



## Security & Surveillance



## Healthcare



## Transportation



## Retail



## Industrial



## Others



Network

# The maritime cyber ecosystem comprises of:

- **Ports** with Cargo handling and Container tracking systems, Shipyard inventories and automated processes,
- **Ships**, the transportation means
- Shipping **companies**
- All of them are relying on Information Systems to function

- Each one if under cyber attack will have an impact on the other(s) and **impact** on **Business Objectives**

**Cyber Risk is a reality**

# IMPACT of CYBER ATTACKS

World Fuel Services (WFS) recently fell victim to a bunkering scam reported to have cost the company an estimated **\$18 million**

Globally, it estimated that cyber attacks against oil and gas infrastructure will cost energy companies close **to \$1.9 billion by 2018.**

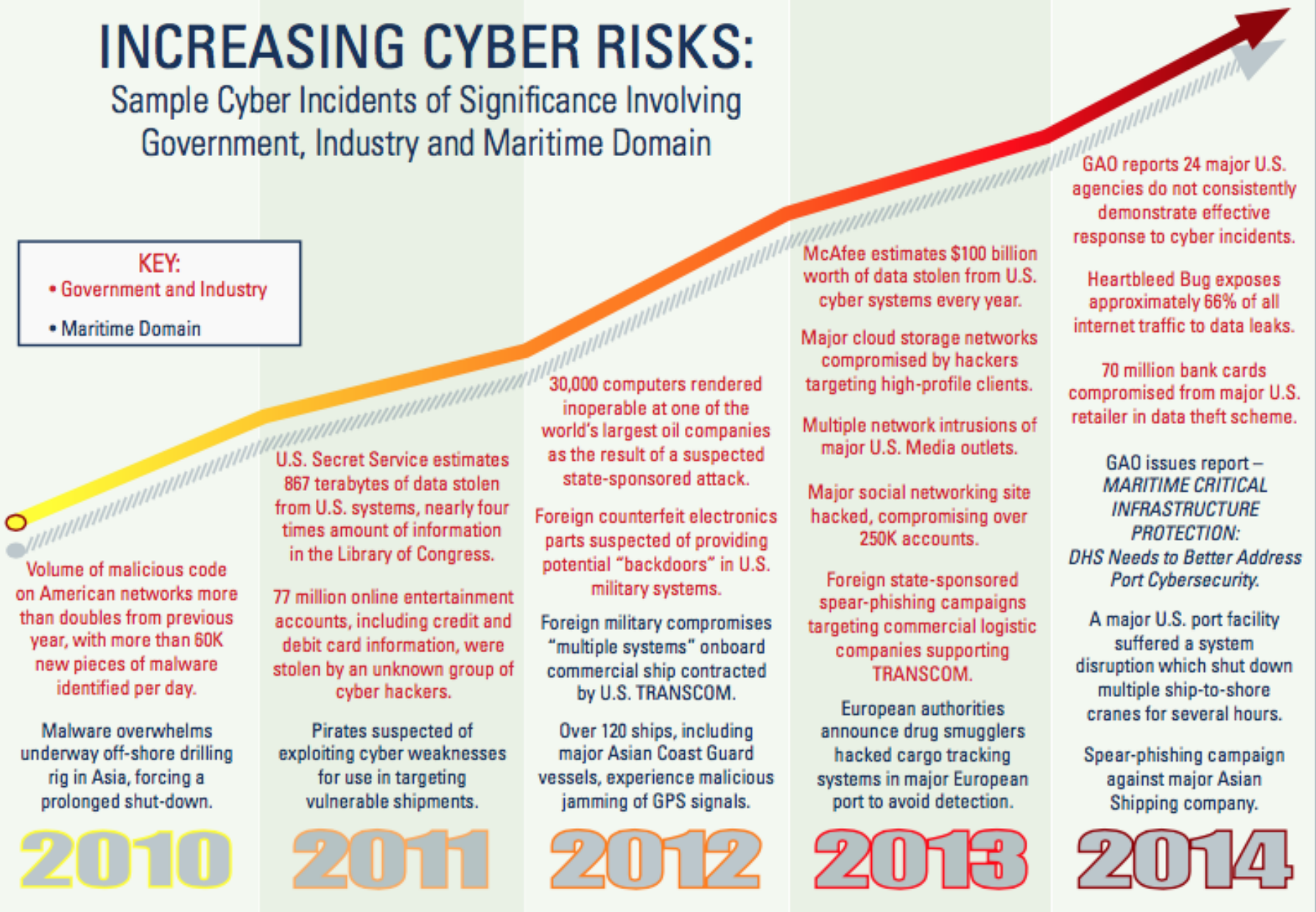
The British government reckons cyber attacks already cost UK oil and gas companies around 400 million pounds (**\$672 million**) a year.

# INCREASING CYBER RISKS:

Sample Cyber Incidents of Significance Involving Government, Industry and Maritime Domain

**KEY:**

- Government and Industry
- Maritime Domain



Volume of malicious code on American networks more than doubles from previous year, with more than 60K new pieces of malware identified per day.

Malware overwhelms underway off-shore drilling rig in Asia, forcing a prolonged shut-down.

**2010**

U.S. Secret Service estimates 867 terabytes of data stolen from U.S. systems, nearly four times amount of information in the Library of Congress.

77 million online entertainment accounts, including credit and debit card information, were stolen by an unknown group of cyber hackers.

Pirates suspected of exploiting cyber weaknesses for use in targeting vulnerable shipments.

**2011**

30,000 computers rendered inoperable at one of the world's largest oil companies as the result of a suspected state-sponsored attack.

Foreign counterfeit electronics parts suspected of providing potential "backdoors" in U.S. military systems.

Foreign military compromises "multiple systems" onboard commercial ship contracted by U.S. TRANSCOM.

Over 120 ships, including major Asian Coast Guard vessels, experience malicious jamming of GPS signals.

**2012**

McAfee estimates \$100 billion worth of data stolen from U.S. cyber systems every year.

Major cloud storage networks compromised by hackers targeting high-profile clients.

Multiple network intrusions of major U.S. Media outlets.

Major social networking site hacked, compromising over 250K accounts.

Foreign state-sponsored spear-phishing campaigns targeting commercial logistic companies supporting TRANSCOM.

European authorities announce drug smugglers hacked cargo tracking systems in major European port to avoid detection.

**2013**

GAO reports 24 major U.S. agencies do not consistently demonstrate effective response to cyber incidents.

Heartbleed Bug exposes approximately 66% of all internet traffic to data leaks.

70 million bank cards compromised from major U.S. retailer in data theft scheme.

GAO issues report – **MARITIME CRITICAL INFRASTRUCTURE PROTECTION: DHS Needs to Better Address Port Cybersecurity.**

A major U.S. port facility suffered a system disruption which shut down multiple ship-to-shore cranes for several hours.

Spear-phishing campaign against major Asian Shipping company.

**2014**

- Traditional Cyber Security is not effective any more.
- Only the “Firewall” and the “Antivirus” are NOT enough to protect your valuable assets on board ships and on the land based company
- “Real Time” detection, dynamic threat protection, signature-less technology across the different stages of attack life cycle.

# PANEL DISCUSSION

- **Katerina Raptaki**, IT Manager, **Navios**
- **Adonis Violaris**, Marketing Director, **Interorient Shipmanagement**
- **Manos Manoli**, IT Manager, **Marlow Navigation**



# WRAP UP

# Take Away

Treat Cyber Risk as a Business Risk  
and  
Cyber Security as an  
Enabler to Business Objectives

THANK YOU

# Cyber Security And Future-Proofing Your IT Infrastructure

Emmanouil CHRISTOFIS

Cyber Defence Capabilities specialist

[e.christofis@yahoo.gr](mailto:e.christofis@yahoo.gr)