A presentation by

HILL DICKINSON

"Back to the Future"
Cyber Crime in the Shipping Industry

Digital Ship
Maritime Cyber Forum, London
4 December 2018

JLT
ST Botolph Building
138 Houndsditch, London

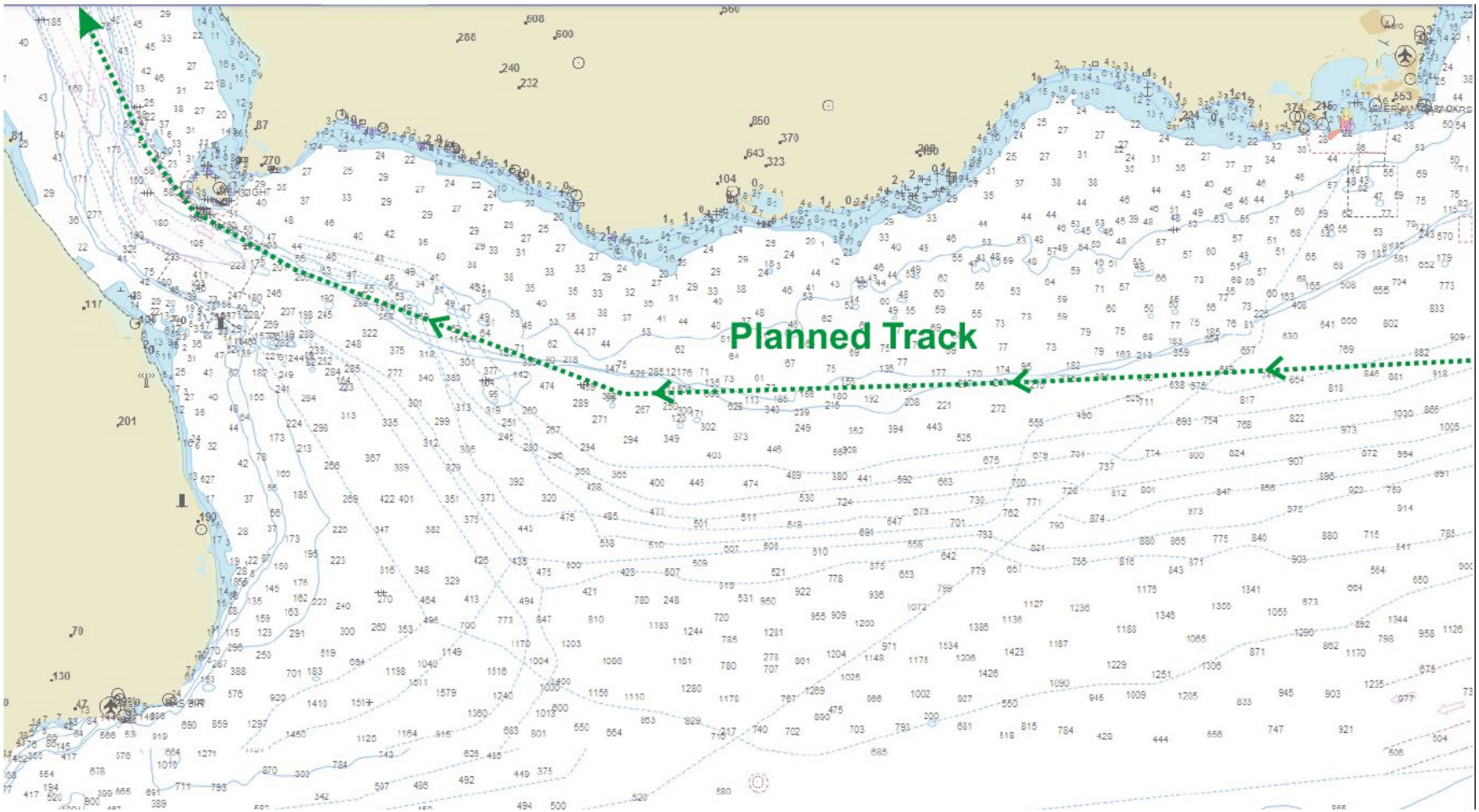
The Incident

- At 04:00 12 August 2018 the head office of the "Amazing Cruise Company" – based in Nassau Bahamas received the following distress call from the master of their cruise vessel MV Wonders:
- *"Mayday Mayday Mayday - this is MV Wonders communicating on all channels. We are under suspected piracy attack. Please advise"*
- The following radio traffic then ensued:
- *"MV Wonders, MV Wonders - this is operations Nassau - please advise current position, speed and nature of attack"*
- *"Operations – we are currently in position Lat 12 degrees 25 minutes North, Long 043 degrees 53 minutes East, we have increased speed to 18 knots and are taking avoidance manoeuvres"*
- *"MV Wonder MV Wonders - your position is noted, we are instigating immediate emergency response and notifying US Naval/Nato - please advise nature of attack"*

- *"Three vessels approaching at speed, two to starboard one to port - vessels appear to be heavily armed. Suspected RPG"*
- *"They have fired RPG – repeat RPG - contact starboard midship's"*
- *"MV Wonders MV Wonders - please advise scope of damage, any casualties ? We are in contact with US Naval authorities"*
- *"MV Wonders MV Wonders - please respond"*
- *"MV Wonders MV Wonders this is operations Nassau - please update position/situation"*
- No further radio traffic is received from the vessel.
- The cruise company immediately activate their emergency response plan which includes notification both to the FBI and US naval authorities. The position of the vessel as notified in the previous message is communicated. This is also verified by remote access to the ships electronic systems.

The Ship's Electronic Systems

HILL DICKINSON



Emergency Response

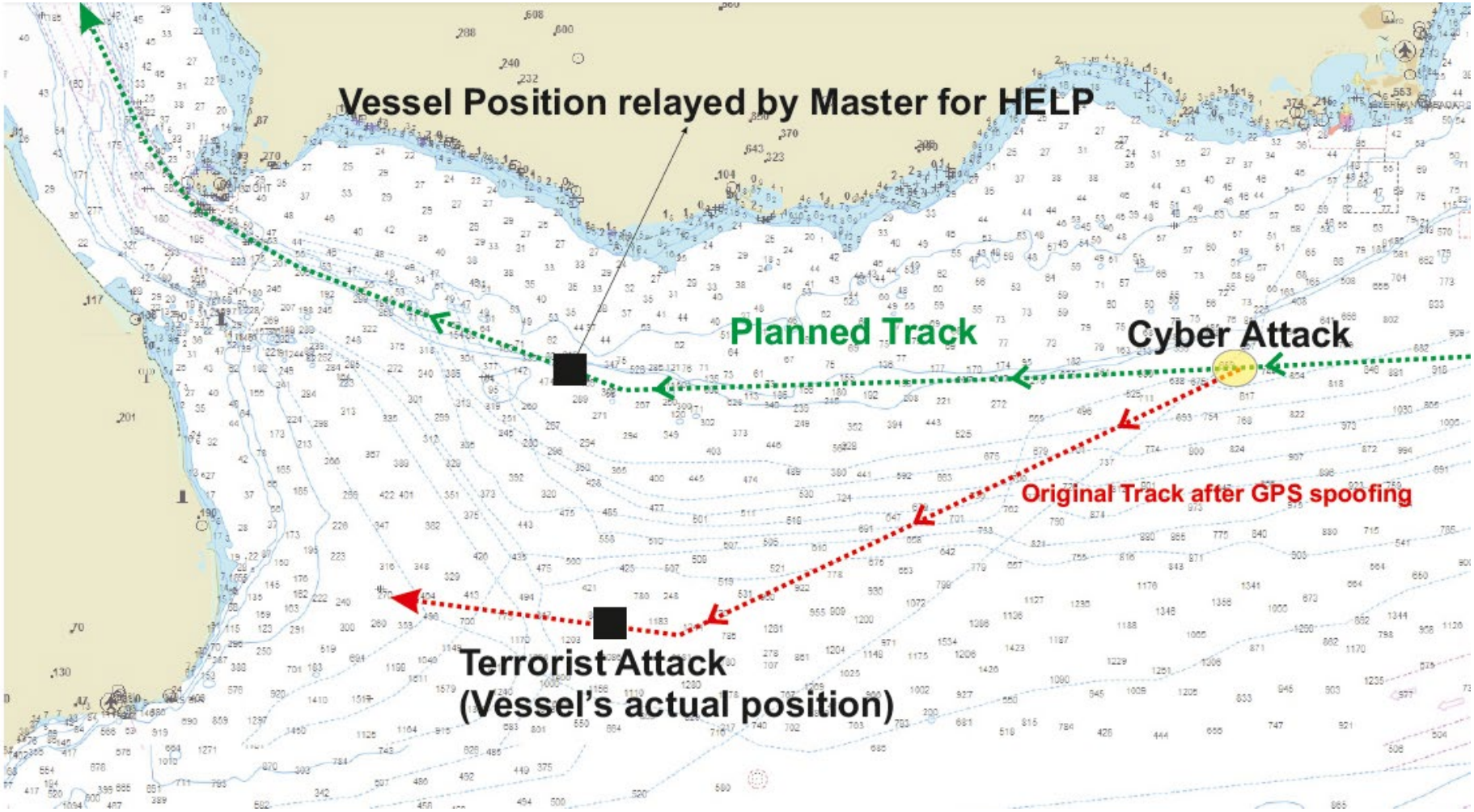
- Despite all attempts to re-establish contact with the vessel no response is received.
- Fortunately a US naval frigate is in the vicinity of the reported attack and proceeds with all speed to attend.
- Upon arrival the US naval frigate advises that there is no sign of the vessel. The frigate launches helicopters to search the area.
- After a one-hour search operating on a GEOREF search pattern the vessel is located.
- Tactical response, which by now includes specialist Navy Seal teams, are dispatched to the actual location

Findings at location

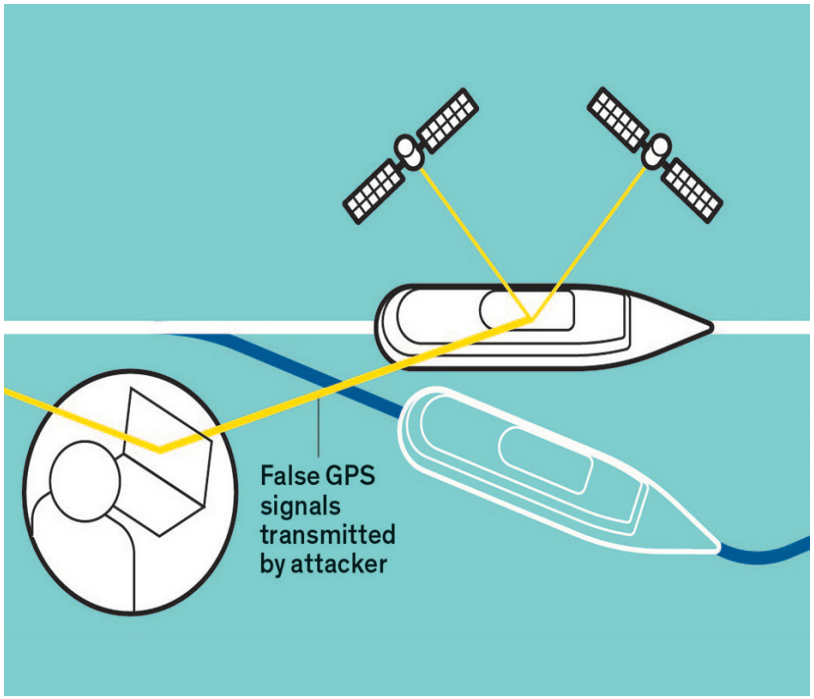
- On attendance it becomes immediately apparent that the motive for the attack is terrorist based.
- Six key members of the crew and a further six passengers have been ritually executed in the vessels main auditorium. Passengers have been forced to watch the executions.
- A check of passenger and crew members shows nine crew and 25 passengers (including some children) are missing. Reports from crew members advise that immediately following the attack a number of passengers and crew members were forced into the launches and taken on board a helicopter which had landed on the vessel during the attack.
- A DVD left playing on the vessels public address system advises that the attack has been carried out by a terrorist coalition in retaliation for the continued atrocities of the West.

HILL DICKINSON

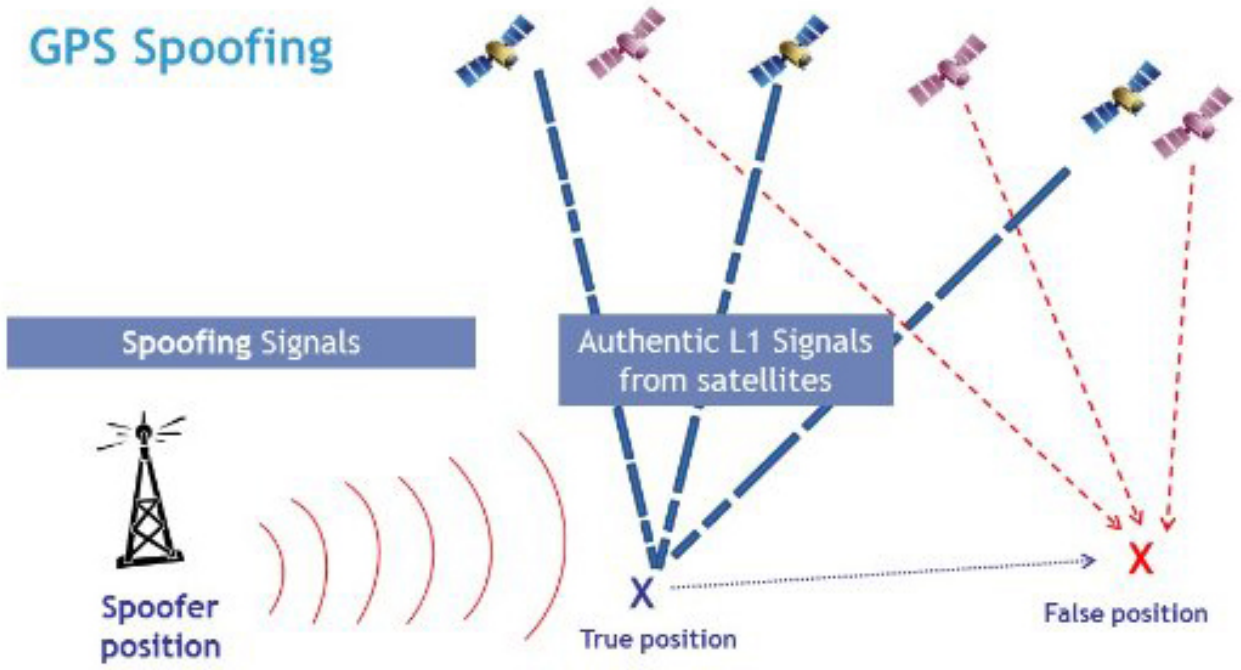
Actual location



How was this achieved (1)



How was this achieved (2)



A Hollywood movie concept or reality?

- The scenario that we have just described may seem far-fetched but;
- The New York Times in 1978 reported how the FBI had arrested four individuals who had planned to seize a cruise vessel based on the Rod Serling novel, “Assault on the Queen" and the subsequent film of the same title starring Frank Sinatra.
- In 2017 a cargo ship travelling from Cyprus to Djibouti lost control of her navigation system for 10 hours preventing the Master from manoeuvring with the intention of steering the vessel into a territory where it could be easily boarded by pirates and robbed. A source later commented that "the entire IT system of the vessel was completely hacked”.
- And then lest we forget …….

USS Cole

Achille Lauro

Twin Towers

HILL DICKINSON

1. Is cybercrime really a big problem?

- The UK government is investing £1.9 billion in cyber-security over the next five years
- The global cost of cybercrime will reach $2 trillion by 2019
- Of 383 organisations asked who suffered at least one data breach in 2016, the average cost per breach was $4 million
- 2017 Report – 5 day loss of GNSS would cost UK £149 million.
- Maersk not Petya

Cont…

- Giles Hunnisett (Master Mariner and consultant with Waves Group) – “what I am looking at more and more is a more widespread problem. ECDIS could have 20,000 vessels, all of them updated by a few companies. Imagine a bug getting into 1,000 ships all at the same time. They would not be able to leave or enter ports or if they were at sea establish exactly where they were. The consequence would be a huge business interruption. The more people I see the more I hear that they are surprised it hasn't happened yet. Meanwhile, on board, we know the danger, but we cannot do anything about it”.
- 2018 Cosco attack
- So significant is the risk that in July 2018 NATO issued requests for reports of instances of GPS or AIS interference in the Mediterranean, noting that in the past few months several electronic interferences had been detected.
- Is the next Achille Lauro, USS Cole and Twin Towers waiting in the wings ?

HILL DICKINSON

2. Impact on the Maritime Supply Chain

- ITIC have recently reported the average cost of a cyber fraud at $120K per attack/incident. Common examples are interception and redirection of cash to master funds, and creating false invoices and accounting details for services such as annual lifeboat certification.

MAERSK CASE 2017:
„Loss of 300M USD in 17 Minutes“
(Andy Jones, former CISO Maersk)

NotPetya:
10.000M USD Global Damage

A Ship is a Collection of:

- **Outdated Systems**
- **Unpatched Systems**
- **Poor Trust Models**

And: Always Connected!

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

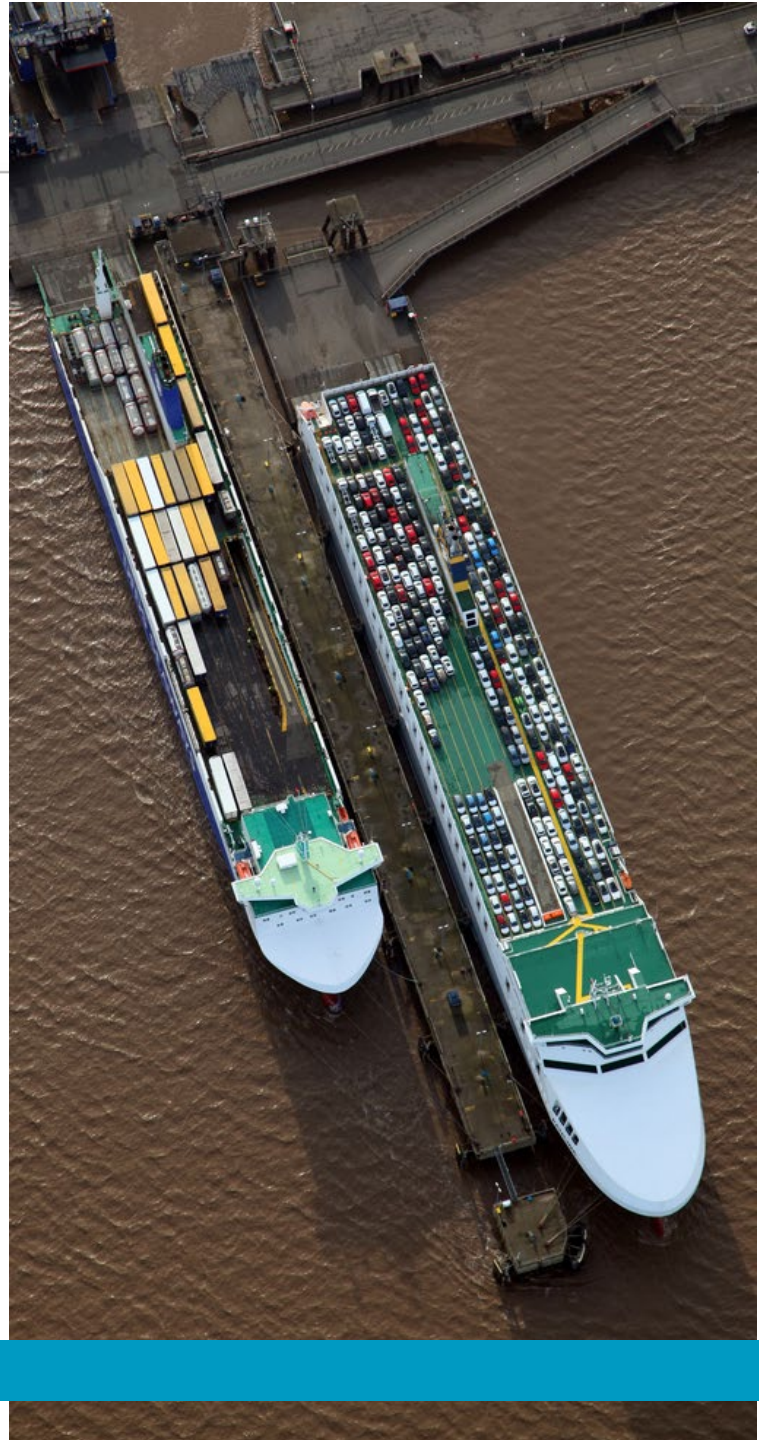
MARAD / MSCI / Alert / 2018-008A-GPS Interference-Jeddah Port, Saudi Arabia

2018-008A-GPS Interference-Jeddah Port, Saudi Arabia

HILL DICKINSON

3. A cybercrime time line

- **2011 –** IRISL services hacked causing damage to rates/loading schedules/delivery schedules/location of boxes (some never traced).
- **2011-2013** – Port of Antwerp – drug cartel – illicit drugs and contraband seized $365 million/firearms seized $1.5 million (led to MSC v. Glencore International AG [CA]).
- **2012** – Australian customs and border protection hacked – inability to trace containers.
- **2012 – 2014** – Danish port authority – email virus led to full shut down and ultimately infected government systems.
- **2014** - Semi Sub Gulf of Mexico destabilised – 19 days to make seaworthy and return to operation. (Similar attacks to other rigs off Africa).
- **2016** – 280 vessels forced to return to port following problems with navigation systems – N.Korea?
- **2017** – 20 ships in Black Sea GPS spoofed – 32km inland of actual position.
- **2018** – COSCO hit by a cyber attack affecting the carriers ability to communicate with vessels, customers and marine terminals.



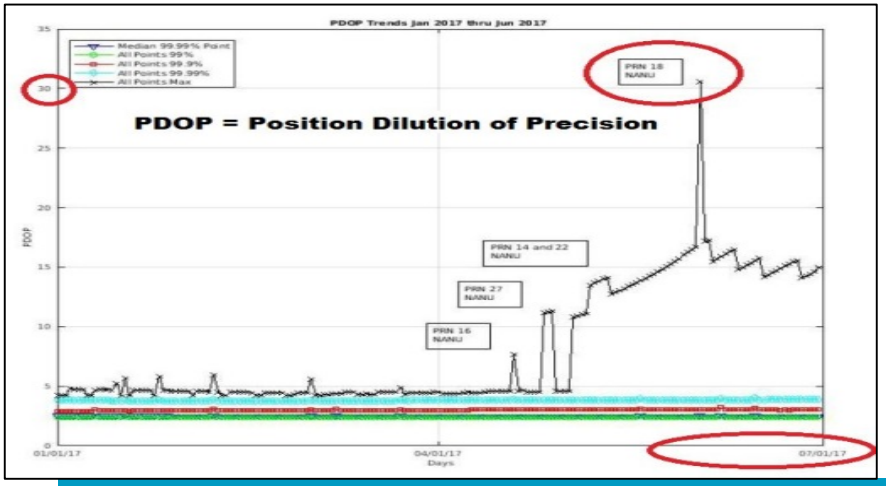
4. Fake news?

- **2017** – 20 ships in Black Sea GPS spoofed – 32km inland of actual position.
- Thanks to Patrick O'Keefe of AMC Solutions

MARAD

2017-005A-GPS Interference-Black Sea

A maritime incident has been reported in the Black Sea in the vicinity of position 44-15.7N, 037-32.9E on June 22, 2017 at 0710 GMT. This incident has not been confirmed. The nature of the incident is reported as GPS interference. Exercise caution when transiting this area.



EGNOS Historical Status Services

Status	Date	Start	Gap End	Gaps
Critical	2017-06-04	03:41:00	03:43:00	120
Critical	2017-06-06	13:07:01	13:11:01	240
Critical	2017-06-18	18:02:26	18:04:26	120
Critical	2017-06-20	07:48:01	08:27:01	2340
Critical	2017-06-20	08:33:01	08:49:01	120
Critical	2017-06-28	09:33:15	09:35:15	120
Critical	2017-06-28	10:18:15	10:21:15	240
Critical	2017-06-28	09:02:15	09:18:16	960

Cybercrime in a maritime legal context

Three central tenets of the traditional concept of the seaworthiness of a vessel:

- First, a ship is seaworthy if she has that degree of fitness which the ordinary careful owner would require his vessel to have at the commencement of her voyage having regard to all the probable circumstances of it. In short, the question is: *would a prudent owner have required it should be made good before sending his ship to sea, had he known of it?*

- Second, a vessel's seaworthiness extends beyond its physical fitness of the relevant voyage. It extends to ensuring that the vessel has (i) sufficient, efficient and competent crew, and (ii) adequate and sufficient systems on board to address matters that might be encountered during the relevant contractual voyage.

- Third, whether a vessel is seaworthy is to be considered by reference to the state of knowledge in the industry at the time.

Viewed against these tenets we can make the following observations;

- in the context of the threat of cybercrime in shipping it will become increasingly difficult for shipowners to argue successfully that the state of knowledge in the industry is such as to permit them to do nothing to address the potential of cyber attacks. Publications from P&I Clubs, the IMO, the "Be Cyber Aware At Sea" campaign, the "Guidelines on Cyber Security On Board Ships" produced by BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO and the IMO's "*Interim Guidelines on Maritime Cyber Risk Management"*
- it is noteworthy that two of the central themes of most of the publicly-available guidance on how to address the risk are described in terms that closely mirror two of the central tenets of seaworthiness – the implementation of cyber risk management systems and protocols (both on shore and at sea) designed to avoid, transfer, and mitigate the risk of cyber-attacks; and the training and education of relevant crew and personnel on the identification and mitigation of cyber-risks.
- In the absence of being able to show positive steps taken in line with either of these themes, a shipowner caught in a hypothetical claim of the type under consideration may well find itself in an uphill battle to establish the seaworthiness of the vessel.

6. How may this impact current legal protection?

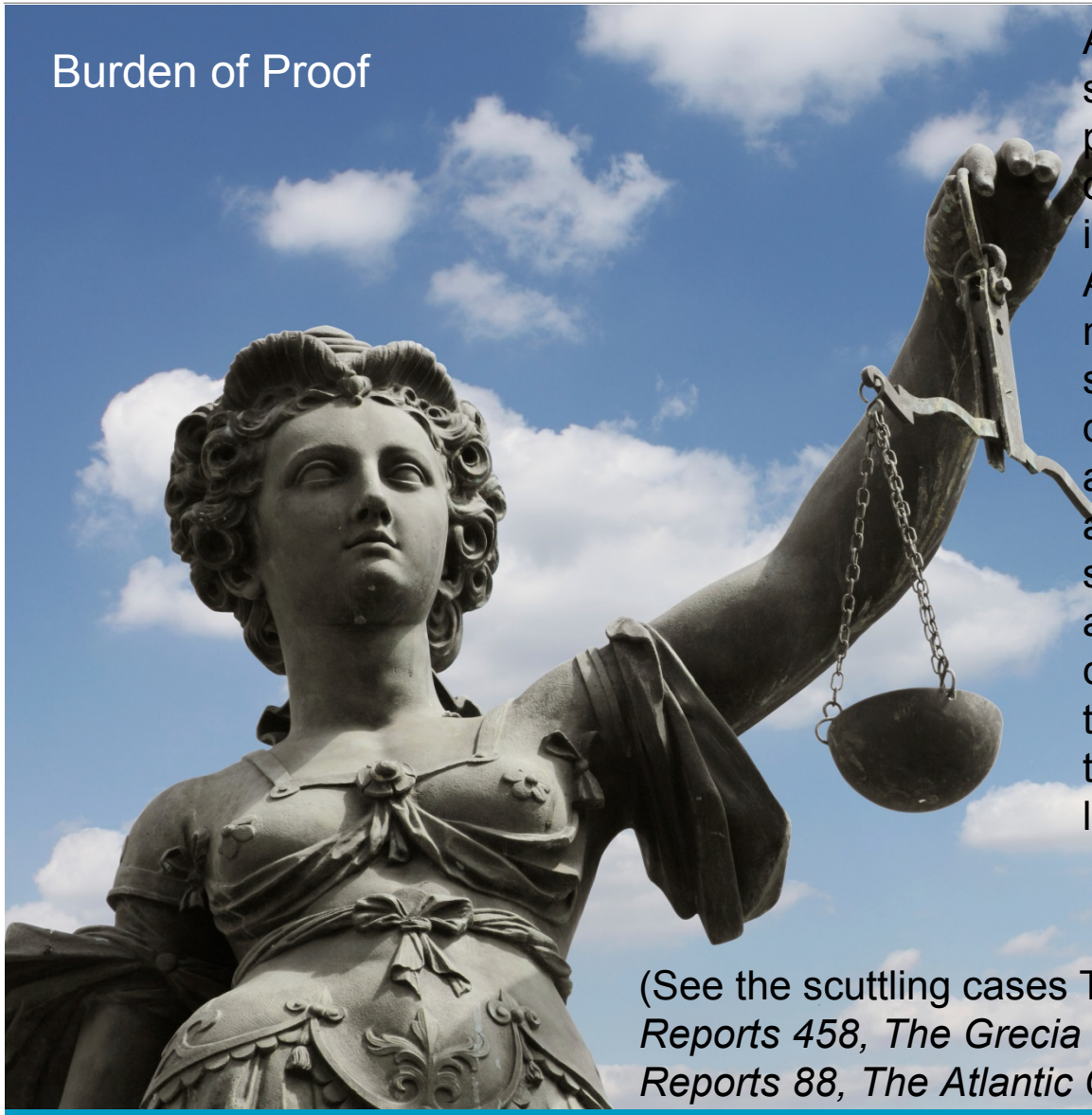
- Limitation of liability
  - 1957
  - 1976
  - 1996 Protocol
  - 2012

- Could our scenario provide grounds to break limit?
  - Art 4 1976 Convention

  "A person liable shall not be entitled to limit his liability if it is proved that the loss resulted from his personal act or omission, committed with the intent to cause such loss, or recklessly and with knowledge that such loss would probably result"

HILL DICKINSON

Burden of Proof



Although technically the civil standard "on the balance of probabilities" applies a number of decisions support the position that in order to meet the test under Article 4 the standard of proof will not fall far short of the criminal standard "beyond all reasonable doubt". Further those seeking to apply the test may not have direct access to all relevant evidence such that the Court may consider all relevant indirect and circumstantial evidence. Further that those seeking to apply the test in order to defeat a right to limit do not need to prove motive.

(See the scuttling cases T*he Milasan [2000] 2 Lloyds Reports 458, The Grecia Express [2002] 2 Lloyds Reports 88, The Atlantic Confidence [2016] EWHC 2412*).

- The Atlantic Confidence [2016] EWHC 2412

HFW – “all this case demonstrates is that in the correct factual scenario the Admiralty Court will be willing to take a decision to break limits”.

- Art 4 1976 Convention

“A person liable s proved that the loss resulted fror ith the intent to cause such loss, loss would probably result”

RECKLESSLEY

The law

Eurasian Dream [2002] I Lloyds Reports 719 – fire on board a car carrier in Sharjah. Owners found in breach of Art III r. 1 of the HVR despite being absolved from intentionally starting the fire and therefore deprived of use of the fire defence Art IV r 2(b).

Inexperience of the master.

Lack of training in risk of cargo operations for car carriers.

An ineffective regime of training and drills.

SOLAS compliance not enough

Extremely basic handover and general induction.

Absence of vessels specific firefighting procedures.

Simply having manuals on board not enough.

7. And although beyond the scope of this session, what about Charterers risks?

- take for example a charterers' obligations in relation to providing a safe port. In circumstances where a vessel suffers damage as a result of a ports cyber security being compromised and it can be shown that the port had inadequate cyber security systems in place, could it be argued that the port is rendered unsafe for the vessel in question?

- in relation to the obligations for safe stowage which often may rest with charterers as a matter of contract, in circumstances where the loading operation is affected due to a cyber-attack could resulting damage, both physical and financial, ultimately be found to be the responsibility of the charterer?

HILL DICKINSON

8. Why us and what can be done?

The maritime sector is looking like a soft target!

- Facing the inevitable Fact: Security is expensive
- Attacks are becoming weaponised / already on the market but not seen as such
- Manufacturers demonstrate poor Cyber-Hygiene
- Global Compliance is just at beginning

WHAT IS NEEDED?

- Threat Modelling of Ships including „Zero Days“
- Penetration Testing of Ships, Ports & Satellite Systems
- Introduction of Monitoring Systems
- Information Sharing between Actors in order to exchange Experience & Cyber Vulnerabilities
- Cyber Response Plans & Training Exercises

IMO

- IMO has issued MSC-FAL. 1/Circ.3 *Guidelines on maritime cyber risk management.*
- The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.
- The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

IMO

- IMO guidelines presented functional elements that supported cyber risk management.
- Identify: To define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
- Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
- Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
- Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

BIMCO

- New cyber security clause in May 2019

8. Conclusion

1. What cyber risks can we identify to ECDIS, AIS and other systems, shipboard and otherwise?

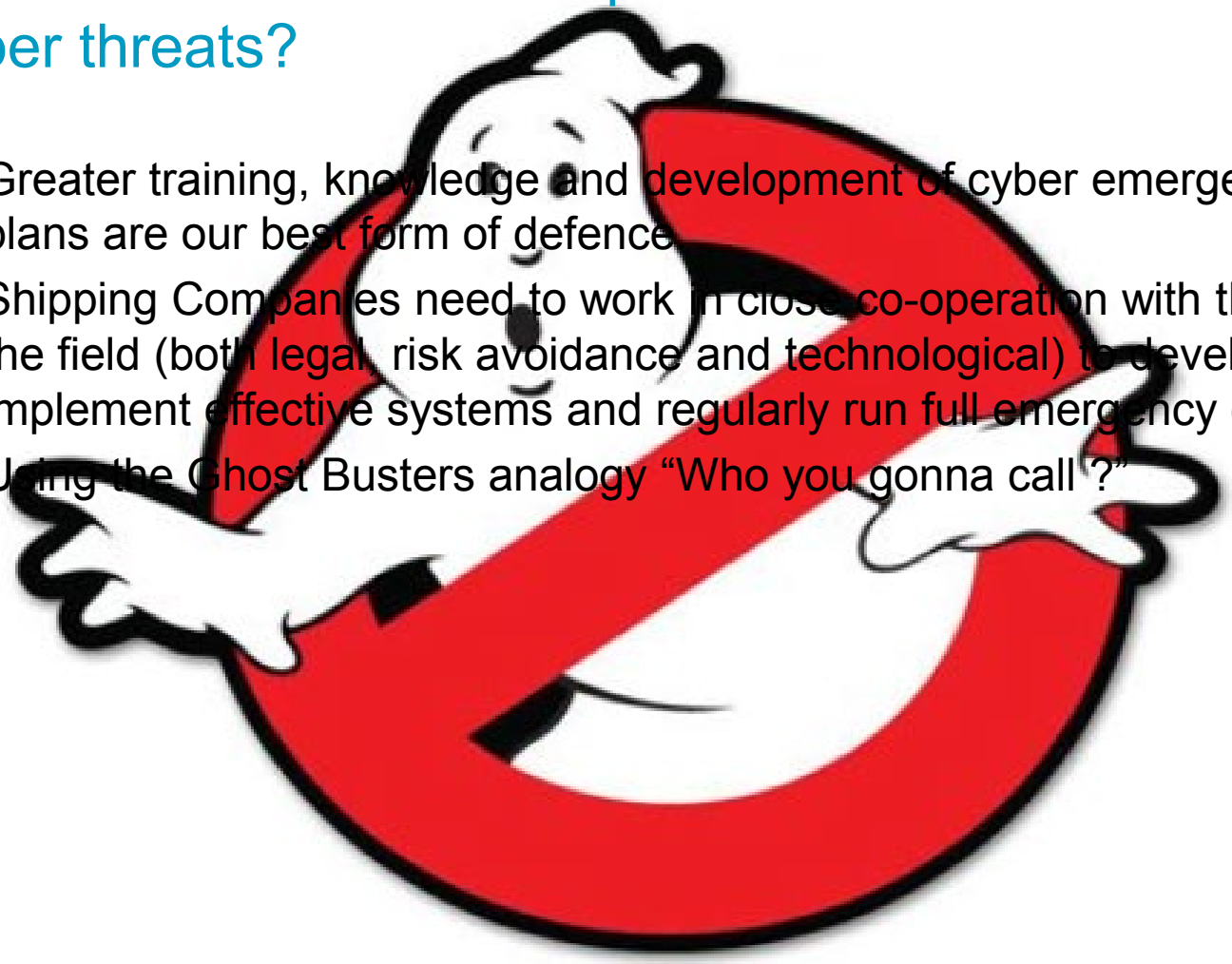
- Both actual incident and detailed expert testing and analysis has revealed that all of these systems (indeed almost all shipboard systems from engine monitoring to smart containers) are exposed to infiltration and cyber attack.
- The scope of the risk is significant and comes from a range of sources and for a range of motives (which is in itself a contributing factor in the significance of the threat).

2 . What are the best ways for owners and crews to protect against cyber risks?

- Take the risk very seriously.
- Guidance and procedures must originate at Board level
- Cyber avoidance risk barriers need to be implemented at every level of the business – not just across the vessels rail but in the owning office – for example, security checks and monitoring of all staff (however junior) that could gain access to electronic systems.
- There must then be in place a rigorous training regime. Not just how to prevent an attack and identify risk but what steps to take as soon as it becomes clear an attack is underway. Quick and effective response can save millions of dollars and more importantly business reputation and potential loss of life.

3. How can we make ships and mariners safe from cyber threats?

- Greater training, knowledge and development of cyber emergency response plans are our best form of defence.
- Shipping Companies need to work in close co-operation with the experts in the field (both legal, risk avoidance and technological) to develop and implement effective systems and regularly run full emergency drills.
- Using the Ghost Busters analogy “Who you gonna call ?”



HILL DICKINSON

Thank you

Any questions?

A presentation by

HILL DICKINSON