A presentation by

HILL DICKINSON

"Back to the Future"
Cyber Risk Revisited

2018 South African MLA
Le Franschhoek Hotel & Spa

Julian Clark
Hill Dickinson LLP

The Incident

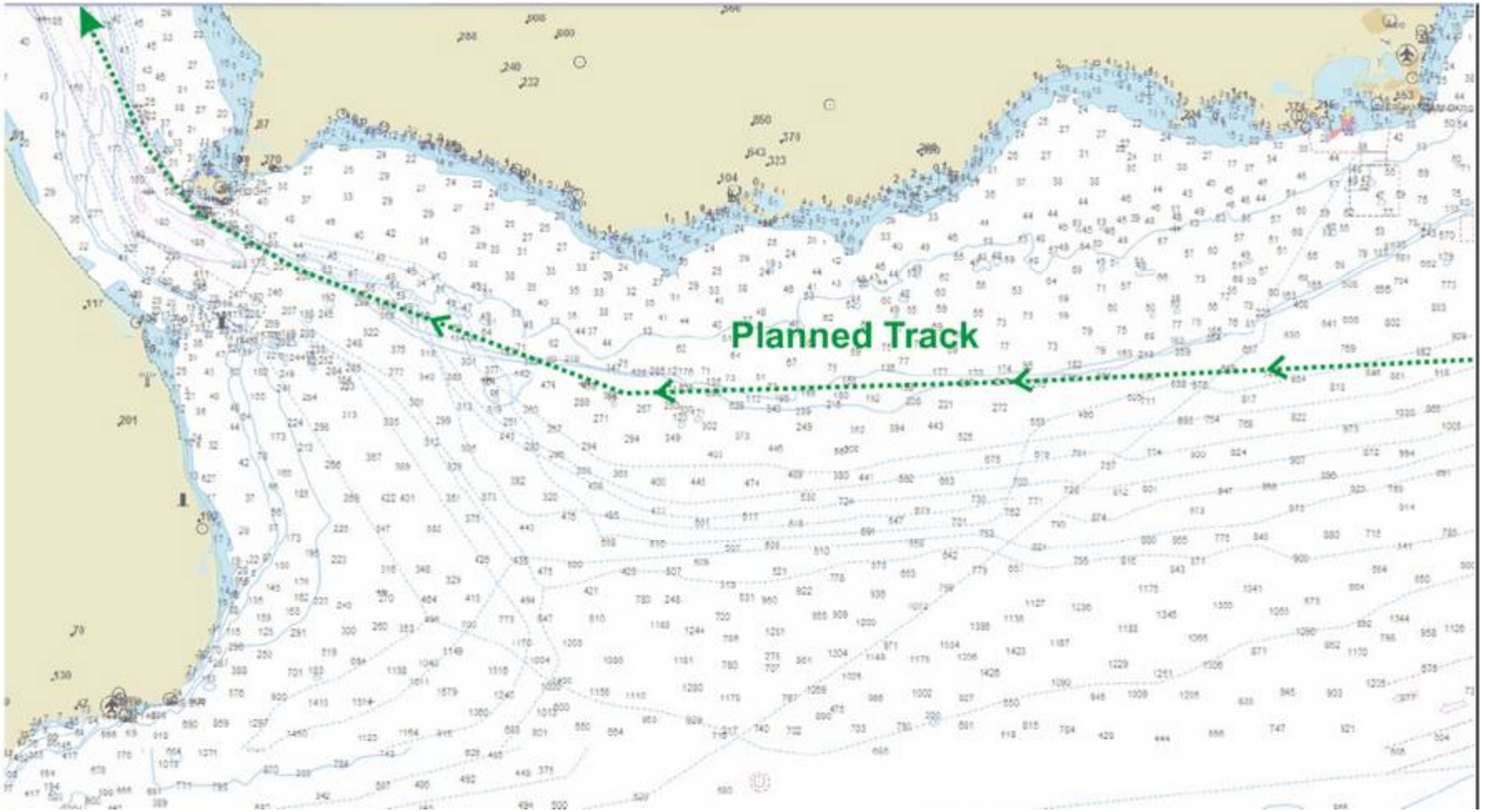
- At 04:00 12 August 2018 the head office of the "Amazing Cruise Company" – based in Nassau Bahamas received the following distress call from the master of their cruise vessel MV Wonders:
- *"Mayday Mayday Mayday - this is MV Wonders communicating on all channels. We are under suspected piracy attack. 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”*
- *sound of large explosion*
- *“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.

HILL DICKINSON

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

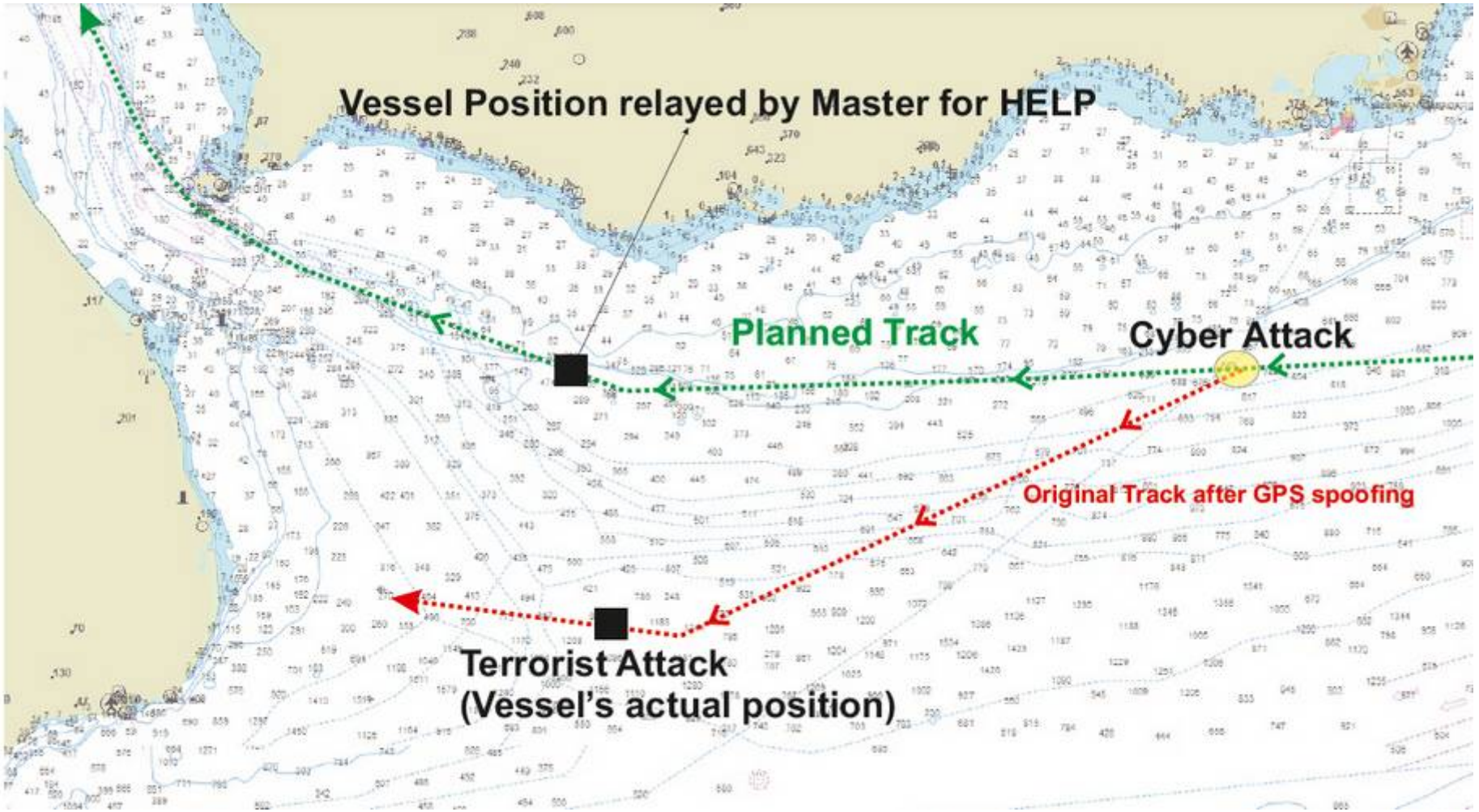
HILL DICKINSON

Findings at location

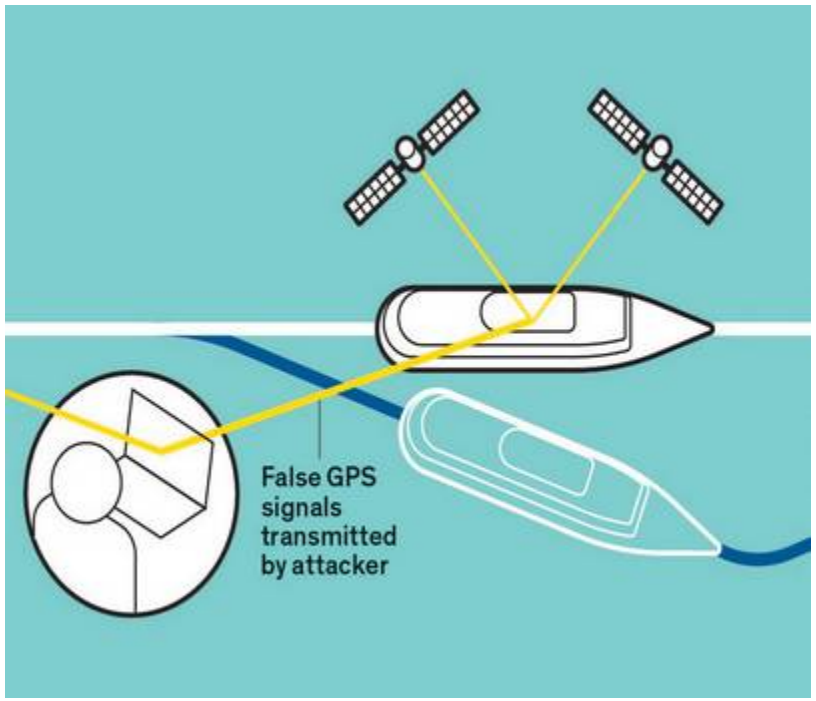
- On attendance it becomes immediately apparent that the motive for the attack is terrorist based.
- Six key members of the crew and a further six passengers have been ritually executed in the vessels main auditorium. Passengers have been forced to watch the executions.
- A check of passenger and crew 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

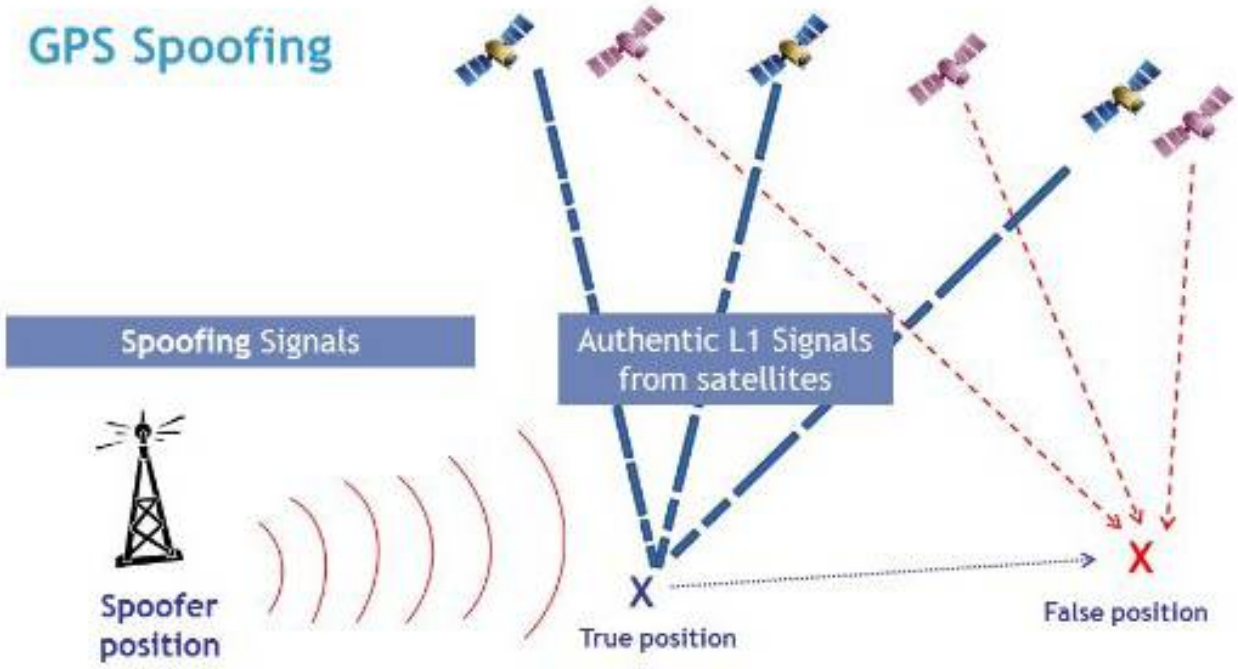
Actual location



How was this achieved (1)



How was this achieved (2)



HILL DICKINSON

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”.
- 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”.

- 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
- In 2017 the International Data Group (IDG) detected 38% more cyber-security incidents than the year before
- 48% of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest

HILL DICKINSON

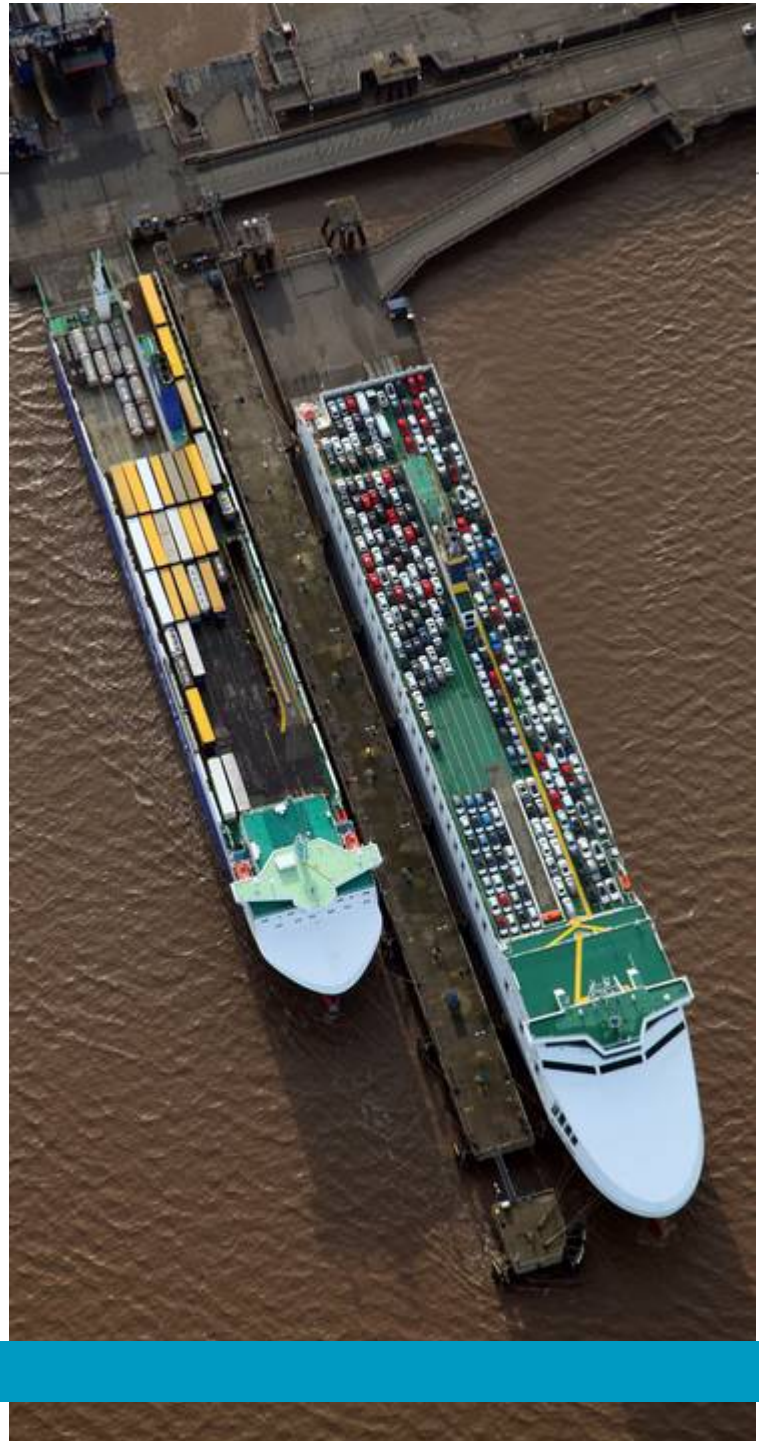
2. Impact on the Maritime Supply Chain

- Hacking into on-line services – including cargo and consignment tracking systems.
- Phishing and links to malware & false web sites.
- Infection via removable media – flash drives.
- Fraudulent Web set up (disclosure of information/reputational damage).
- 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.
- Hacking into navigational systems (ECDIS)
- AIS/GPS Spoofing
- Impersonation Fraud

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.



HILL DICKINSON

4. Examples of specific risks and their consequences to the shipping industry

GNSS Jamming and AIS spoofing.

- Jamming devices cost as little as $100
- AIS/GPS spoofing can be achieved with a $100 VHF set
- Estimated 250,000 cell towers in Russia are equipped with GNSS jamming devices.
- GPS jamming trial – Flambrough Head – showed effect was to create incorrect data on ECDIS, AIS and Radar – all systems !
- Issues with AIS

➢ No authentication protocols;

➢ Easy ability to impersonate targets (ships);

➢ Unencrypted messaging;

➢ Jammers have radius of over 30km.

HILL DICKINSON

4. Examples of specific risks and their consequences to the shipping industry cont.

- 2017 Report – 5 day loss of GNSS would cost UK £149 million.
- 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.

HILL DICKINSON

5.1 Examples of specific risks and their consequences to the shipping industry

Unseaworthiness

- *F.C. Bradley & Sons -v- Federal Steam Navigation* (1926) 24 L1.L.Rep. 446 – definition of seaworthiness - the ship 'must have that degree of fitness which an **ordinary careful and prudent owner** would require his vessel to have at the commencement of her voyage having regard to **all the probable circumstances** of it'
- *Kopitoff -v- Wilson* (1876) 1 QBD 377 – 'fit to meet and undergo the perils of sea and other incidental risks to which of necessity she must be exposed in the course of a voyage'
- *"EURASIAN DREAM"* [2002] 1 Lloyd's Rep. 719 – requires the crew to be adequately trained
- *ISPS/(US) MTSA* 2002 – requires ports to implement security protocols but are not designed with cyber attacks in mind

HILL DICKINSON

5.2 Examples of specific risks and their consequences to the shipping industry

Unseaworthiness cont.

- 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 the voyage having regard to all the probable consequences of it. Would a prudent owner have required it should be made good before sending to sea had he known of it?
  - Extends beyond physical fitness to (i) sufficient, efficient and competent crew (ii) adequate and sufficient systems on board to address matters which may arise during the voyage.
  - By reference to the state of knowledge in the industry at the time.

- Luke Parsons QC & Julian Clark concluded, “in the absence of being able to show positive steps taken in line with implementation of cyber risk management systems and protocols an owner will face an up hill struggle in establishing seaworthiness”

HILL DICKINSON

6. Examples of specific risks and their consequences to the shipping industry

Malware – Not Petya

- Port of LA, Clarksons and Maersk – most high profile.
- Clarksons – 6% drop in share value
- Maersk:
  - Estimated $300 million loss;
  - Congestion in over 80 ports;
  - Replaced 4,000 servers, 45,000 PC's and 2,500 applications;
  - Networked fleet successfully isolated.
- COSCO attack - full financial implication presently unclear

HILL DICKINSON

6. Examples of specific risks and their consequences to the shipping industry

Hacking and beyond

- Change of manifests – illicit goods trade (Port of Antwerp), to mis-description (CHC/Liquefaction risk/Sanctions avoidance).
- Business disruption and reputational damage.
- A new route to industrial espionage.
- Potential to disrupt a Blockchain ?
- **AND WHAT ABOUT THE THINGS THEY DON'T TELL US ABOUT ???**

HILL DICKINSON

7. Cyber and litigation risk

- The Washington DC scandal
- No longer just tipex on the log books
- Needle in the haystack approach to discovery
- GDPR (25 May 2018) E20 million of 4% of global turn over whichever greater.
- GDPR and new Regulation will enforce cyber hygiene. USA implementing legislation to penalise companies for inappropriate data handling and storage.
- ICCA/New York City Bar/CPR Institute working group on cyber security for International Arbitration:

➢ Draft protocol open until 31 December 2018 launched at ICCA 2018 in Sydney;
➢ Protection of digital information in arbitration;
➢ Identifying and protecting the weak link;
➢ Powers to order cyber security measures;
➢ Framework for adopting cyber security measures during the process.

- Why ? High value, high stakes, sensitive and potentially damaging information access.

HILL DICKINSON

Law Firm Exposure – Are you ready to deal with a cyber attack?

- **Law Firm essentials:**
- a data breach plan with step-by-step actions
- procedures to regularly rehearse the plan with all staff
- a designated person responsible for handling any breach
- regular updates concerning the plan to ensure all senior staff are fully familiar with it
- prepared notification messages to 3rd parties and suppliers
- in the UK gathering of evidence for the Information Commissioner to show how the breach has been handled. Similar information gathering for any international regulatory authority.
- regular cooperation with any cyber insurance provider for guidance and in order to ensure maintenance of cover
- pre-prepared statements to customers advising how the firm will deal with any damage
- a no tolerance party to ransom demands

Law Firm Exposure cont.

- **And when an attack takes place:**
- identify where the demand or ransomware originated and how this entered the system
- isolate all infected devices (immediately take them off-line)
- assess how many and which devices have been affected
- restore lost data from backups
- advise customers if their data has been compromised
- once the attack is under control - prepare a "lessons to be learned" review.

HILL DICKINSON

In conclusion

I was recently asked a series of questions on behalf of IHS for their publication – “Safety at Sea”. I believe that my response to those questions serve as an appropriate conclusion to this presentation.

1. What cyber risks do you 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). At the low level (on one view) hackers are attracted to shipping as it represents a challenge to their range of expertise and yet can be perceived by them as less of a life threatening threat for them to interfere with (compared say with hacking into and disrupting flight paths). This however is a misconception on their part as can be identified by the example of destabilisation of an oil platform which not only lead to $100,000's of shut down costs but raised a significant risk of a major incident on the level of Piper Alpha, At the other end of the scale are the cyber terrorists and hactivists – here significant financial disruption and potential loss of life may well be their aim. We live in the shadow of the modern day USS Cole or Achille Lauro.

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

- Take the risk very seriously. In fact make it number one on your risk list. Guidance and procedures must originate at Board level – not left to the IT department or even those routinely dealing with ISPS. 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. **Can technology always solve technology? What is the human, systemic and societal element?**

- If you are asking “is it simply a matter of developing better fire walls etc.?” the answer is no. Again this is why a response and culture from the top of the company down needs to be developed. All owners, operators and those engaged in the logistics chain are now involved (like it or not) in a chess game with that hooded figure we often see in cyber risk power points and presentations. It’s a matter of constantly trying to think 5 moves ahead – how is my business at risk, what could someone gain by attacking my business, do I have the response plans in place to deal with an attack ?

4. **How much of a problem do you see cyber security as being in the short and long term?**

- It is the single largest threat facing international shipping today.

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

- It is unlikely that you will ever be able to eradicate the risk completely. 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 ?”

6. What are the financial risks and solutions?

- I think I have probably dealt with solutions above. As to financial – HUGE – look at the recent publicised examples and remember we are only seeing the tip of the ice berg in what is actually being reported compared to the number and significance of the attacks taking place.

HILL DICKINSON

Thank you

Any questions?

A presentation by

HILL DICKINSON