COMITÉ MARITIME INTERNATIONAL

THE CHALLENGING CONVERGENCE OF MODERN TECHNOLOGY CYBERCRIME AND MARINE INSURANCE

COMITÉ MARITIME INTERNATIONAL

WELCOME!

TOM BIRCH REYNARDSON
CHAIR OF IWG ON UNMANNED SHIPS
BIRCH REYNARDSON & CO
tbr@birchreynardson.com

COMITÉ MARITIME INTERNATIONAL

THE WORK OF THE CMI
COLREGS AND SOLAS
IMPLICATIONS OF THE COLLISION

HENRIK RINGBOM

Professor II, Scandinavian Institute of Maritime Law, Faculty of Law, University of Oslo, Adjunct Professor (Docent) in Maritime Law and the Law of the Sea, Åbo Akademi University, Turku/Åbo,Finland.

Autonomous Ships
– COLREGS and SOLAS implications

Henrik Ringbom
Professor II, Scandinavian Institute of Maritime Law, University of Oslo
Adjunct Professor (Docent), Åbo Akademi University

CMI Event
THE CHALLENGING CONVERGENCE OF MODERN TECHNOLOGY, CYBERCRIME AND MARINE INSURANCE
IMO, **London**
9 November 2018

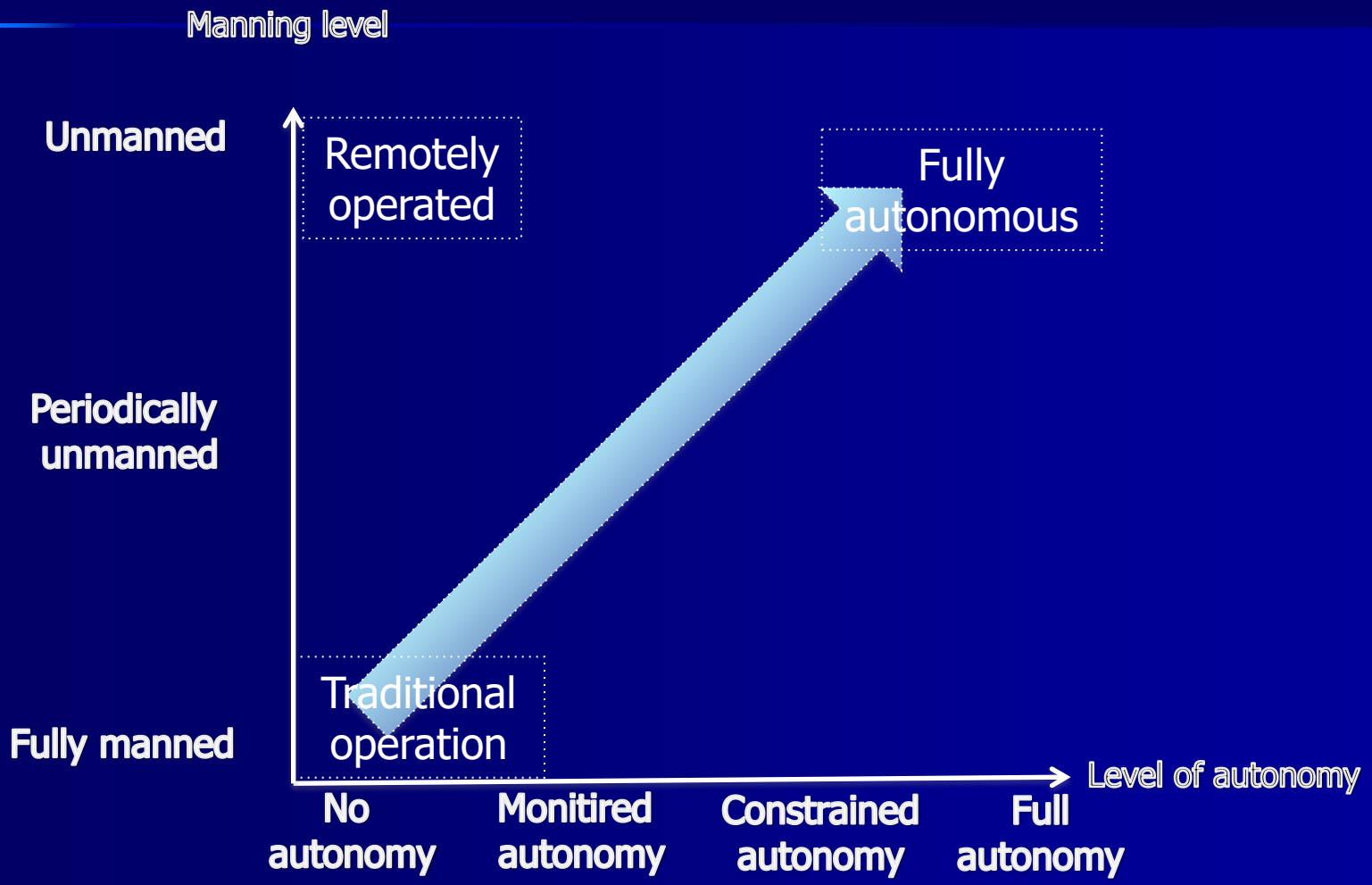
Outline

1. General
2. How lawful is AUTOSHIP today?
   - A. General
   - B. SOLAS: Can it operate in the first place?
   - C. COLREGS: the inherently human touch
3. On-going regulatory work (IMO)
   - A. MASS
   - B. Regulatory scoping exercise
   - C. Different committees
4. Concluding remarks

General

- Unmanned / autonomous ships
- CMI study (MSC 99/INF.8)
- Main legal hurdles
  - Surprisingly few outright conflicts (STCW Part VIII)
  - A lot of uncertainties (function-driven requirements)
  - Affects how you deal with them

Separating autonomy and manning



General

- Unmanned / autonomous ships
- CMI study (MSC 99/INF.8)
- Main legal hurdles
  - Surprisingly few outright conflicts (STCW Part VIII)
  - A lot of uncertainties (function-driven requirements)
  - Affects how you deal with them

SOLAS

- Equivalences & exemptions
- Safe manning?
  - Technology neutral rules (V/14) and guidelines
  - Could safe manning be 0?

SOLAS

- Equivalences & exemptions
- Safe manning?
  - Technology neutral rules (V/14) and guidelines
  - Could safe manning be 0?

Colregs

- **Lookout (Rule 5)**
  - **Sight and hearing**
  - **The 'elephant ear' SOLAS V**/19(2.1.8)
- **"Ordinary practice of seamen" (Rule 2)**

Colregs

Look-out (Rule 5)

Every vessel shall at all times maintain a proper look-out by sight and hearing as well as by all available means appropriate in the prevailing circumstances and conditions so as to make a full appraisal of the situation and of the risk of collision.

Responsibility (Rule 2a)

Nothing in these Rules shall exonerate any vessel, or the owner, master or crew thereof, from the consequences of any neglect to comply with these Rules or of the neglect of any precaution which may be required by the ordinary practice of seamen, or by the special circumstances of the case.

What is happening at IMO?

- Regulatory Scoping Exercise
- Broad discussions at MSC 99 (May 2018) (four degrees of autonomy)
- Correspondence group worked on methodology inter-sessionally over the summer
- Next MSC discussions in December
- LEG 106 in March 2019
- Role for the CMI?

IMO degrees of autonomy

1) Ship with automated processes and decision support

2) Remotely controlled ship with seafarers on board

3) Remotely controlled ship without seafarers on board

4) Fully autonomous ship

IMO degrees of autonomy

1) Ship with automated processes and decision support

2) Remotely controlled ship with seafarers on board

3) Remotely controlled ship without seafarers on board

4) Fully autonomous ship

COMITÉ MARITIME INTERNATIONAL

LIABILITIES FOR OTHER VESSEL COLLISION DAMAGE

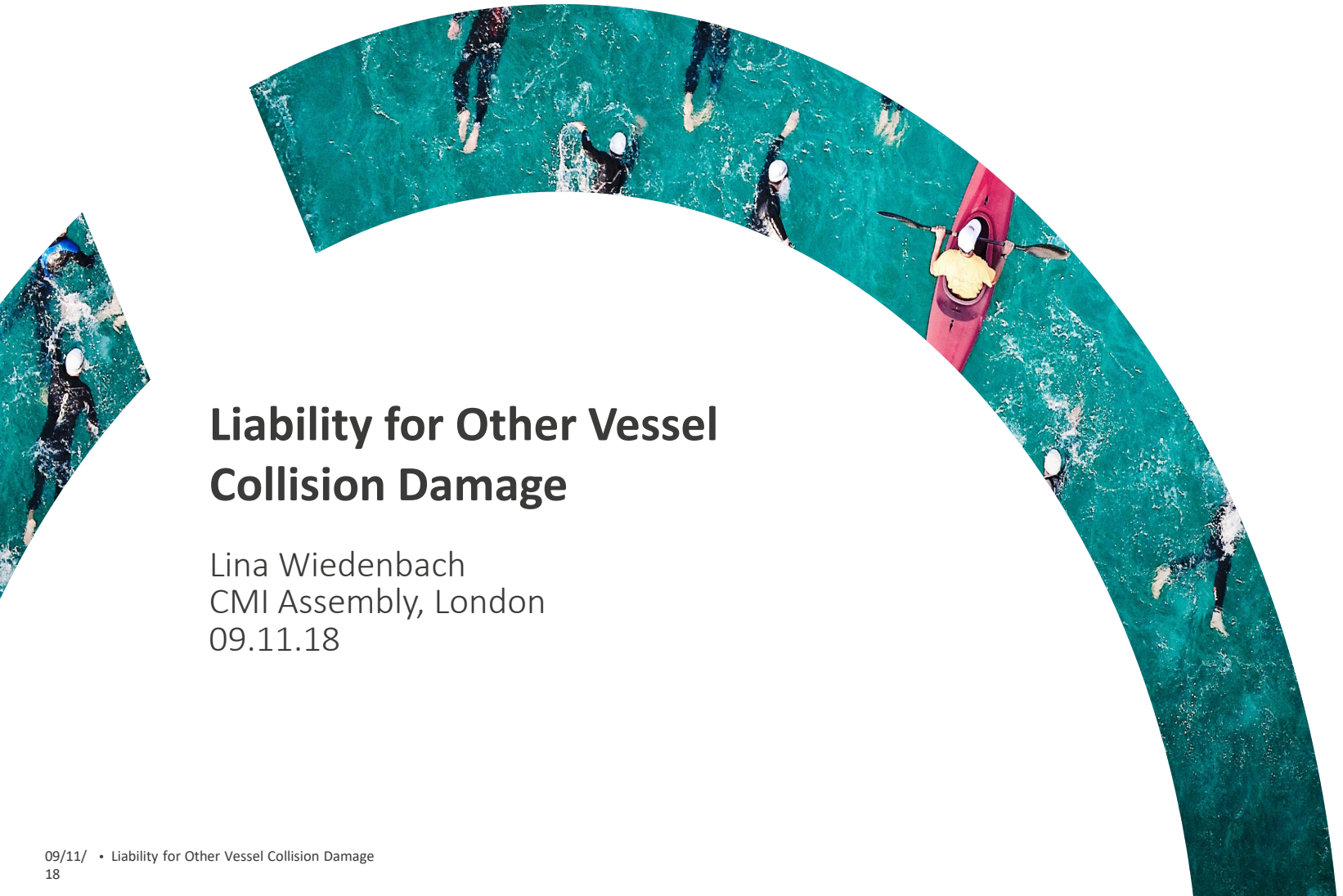
AND

CROSS LIABILITIES OF VESSELS

LINA WIEDENBACH

Arnecke Sibeth Dabelstein, Hamburg

ARNECKE



Liability for Other Vessel Collision Damage

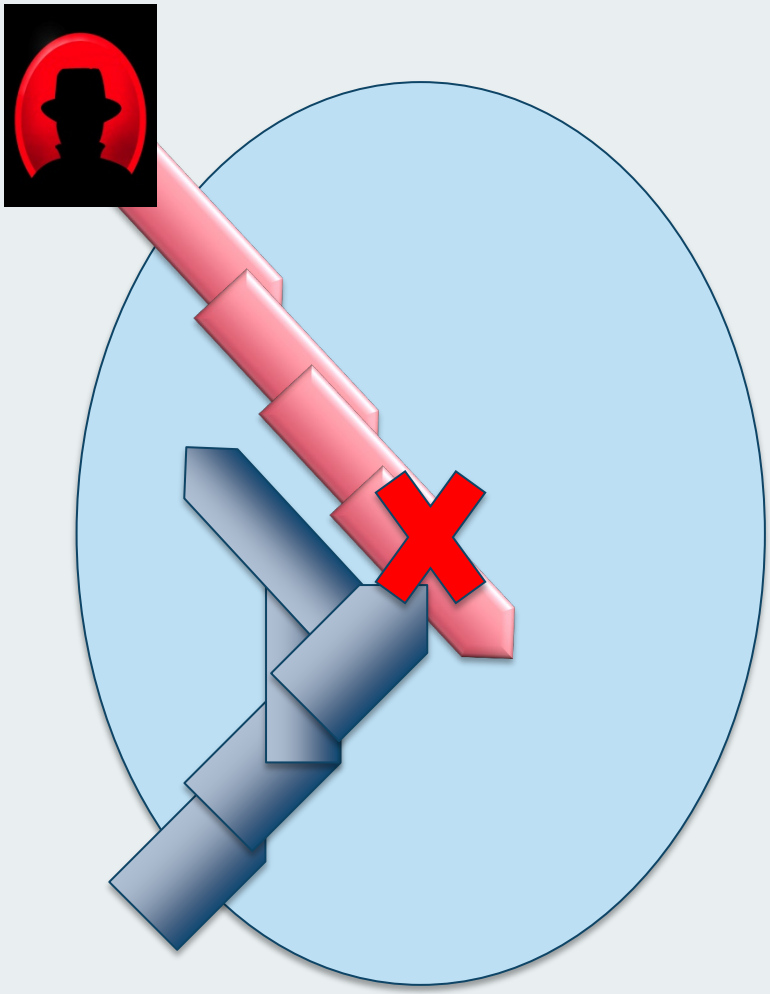
Lina Wiedenbach
CMI Assembly, London
09.11.18

ARNECKE SIBETH DABELSTEIN

Content

ARNECKE SIBETH DABELSTEIN

The Collision and Potential Causes



AUTOSHIP

- Failure to give-way and several other breaches of COLREG (e.g. Arts. 5, 6, 8, 15, 16)
- Infiltration of software provider
- (Possible) Insufficient design security safeguards at London Control Centre

MANDSHIP

- Failure to take actions as stand-by vessel (COLREG Art. 17)
- Infiltration of software provider
- Firewall broken through while crew played video games against shipowner‘s standing instructions
- Inadequate fire wall protection

ARNECKE SIBETH DABELSTEIN

The Current Fault-Based Liability Regime

1910 Collision Convention

- Collision between sea-going and/or inland navigation vessels flying the flag of two different member states
- Wide implementation also outside the direct scope of application (see for example Summary of Responses to CMI Questionnaire on Unmanned Ships)
- Fault-based liability → each vessel liable in proportion to fault (Art. 3)
- However:
  - If none to blame ("event outside the ship") → each party carries its own loss (Art. 2)
  - If not possible to establish the proportion of fault of each vessel → 50/50 (Art. 4)

ARNECKE SIBETH DABELSTEIN

The Current Fault-Based Liability Regime

"By the fault of a vessel" (Arts. 3 and 4)

- Vessel as such cannot be in fault (exception: Netherlands!) – only individuals
- Combined impact of relative culpability and relative causative effect
- Culpability: Negligence as a minimum
  - Negligence in UK law: "the breach of a recognised duty of care owed to a person who may reasonably be foreseen to suffer loss as a direct result of that breach"
  - "Fahrlässigkeit" in German law: "failure to exercise reasonable care in the particular area of activity"
  - "Vårdslöshet / uagtsomhed in "Scandinavian law": Assessment based on four components (1) the risk for damage, (2) the size of the anticipated damage, (3) the possibility to avert the damage, and (4) the damaging party's (objective) possibility to realise the risk for damage

ARNECKE SIBETH DABELSTEIN

The Current Fault-Based Liability Regime

"By the fault of a vessel" (Arts. 3 and 4)

- Guidance for standard of correct action
- Negligence in **navigation** of the ship (e.g. COLREG)
- Negligence in the **management** of the ship (e.g. STCW, SOLAS etc.)
- Shipowner liable for own negligence
  - Directing mind and will of the of the company (cf. Art. 4 LLMC)
  - Exceptionally also person statutorily required to act for company, when that person fulfils the company's obligations e.g. "Designated Person" under the ISM Code
- Shipowner's vicarious liability (employees and other agents) and limits of vicarious liability (usually does not extend to individual contractors)

ARNECKE SIBETH DABELSTEIN

The Current Fault-Based Liability Regime

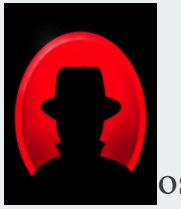
"By the fault of a vessel" (Arts. 3 and 4)

- Causative effect: Fault as cause in relation to damage needs to be:
  - Neccessary ("but for" test),
  - Sufficient (primary cause(s)), and
  - Foreseeable (remoteness test)
- Difficult to establish causal link between negligence and damage, where fault far back in time as will often be the case for MASS

> *Where, as in the present case, the damage sued for is consequential damage said to result from the prior negligence of another or other vessels, it seems obvious that the more remote that prior negligence is, whether in time or space, the more its causative potency must diminish until eventually it disappears altogether (the "Miraflores" and the "Abadesa" Lloyd's Law Reports , [1966] 1 Lloyd's Rep. 97)*

ARNECKE SIBETH DABELSTEIN

Applied to the Present Scenario (MASS and Fault)



No human negligence

ossible negligence of software provider or yard but not attributable to shipowner

(Possible) Negligence in management

No human negligence

Possible negligence of software provider or yard but not attributable to shipownowner

Shipowner vicarious liability for crew‘s negligence in management but causative?
Negligence in management but causative?

AUTOSHIP

- Failure to give way and several other breaches of COLREG (e.g. Arts. 5, 6, 8, 15, 16)
- Infiltration of software provider
- (Possible) Insufficient design security safeguards at London Control Centre

MANDSHIP

- Failure to take actions as stand-by vessel (COLREG Art. 17)
- Infiltration of software provider
- Firewall broken through while crew played video games against shipowner‘s standing instructions
- Wholly inadequate fire wall protection

ARNECKE SIBETH DABELSTEIN

Conclusions and Reflections

#1 Fault Based System Problematic in Relation to MASS

- Due to how decisions are taken at a distance from the ship in time and space
  - Negligence: Shift from negligence in navigation to negligence in management = shift from measure according to COLREGS "dos" or "don'ts" to the general principles and objectives of SOLAS
  - Causation: The more remote the prior negligence is, whether in time or space, the more its causative potency must diminish until eventually it disappears altogether
- Limits of Shipowner's vicarious liability

ARNECKE SIBETH DABELSTEIN

Conclusions and Reflections

#2 Certain Situations (Arguably) not Covered by Current Regime

- 1910 Convention drafted based on the assumption that collision is either due to the fault of one or more involved vessel(s) (Art. 3 and 4) or an event "outside of the ship" (Art. 2) – not due to the fault of third parties acting in a distance from the ship in time and space
- Wording does not fit situation that cause of collision known (→ not Art. 2) but not attributable to the fault of either vessel (→ not Art. 3 or 4)
- Under the current wording how would the courts apportion damage in such situation?
  - Each party bear its own damage (in analogy with Art. 2)?
  - 50/50 split (in analogy with Art. 4)?
  - Or application of national rules for distributing damage, given that the wording of the 1910 Convention strictly read does not seem to cover situation?
  - UNFORESEEABILITY

ARNECKE SIBETH DABELSTEIN

Conclusions and Reflections

Possible Alternative Methods for Distributing Damage

1. Extend circle of persons for whose fault shipowner liable (cf. pilot)

2. Strict liability for MASS

   – Collision between two commercial insured parties not the typical situation where legislator would usually adopt strict liability

   – Delimitation issues foreseeable. How to define and distinguish damage being the result of the realisation of risks emanating from the particular operational risk of MASS from other dangers emanating from the operations of ships. (Strict liability for any damage caused by the ship an option but very far-reaching!)

   – What exceptions shall be made available to the Owner

     – Wilful acts of third parties (cf. the IMO Liability Conventions)?

     – Claimant's contributory negligence?

Conclusions and Reflections

Possible Alternative Methods for Distributing Damage

3. The Doctrine of Risk (cf. Hoge Raad, Netherlands 2001, ECLI:NL:PHR:2001:AD3922) = Wide interpretation of "fault of vessel"

   – Strict liability for the realisation of *"a special risk that has been created because the property does not meet the requirements to be imposed on it in the given circumstances"*

   – Would include particular risks emanating from MASS operation but not be limited to

   – Also the fault of the non-MASS collision opponent would be assessed by same standard

4. "Traffic law solution" – Mixture of strict and fault liability

   – Apportionment based on degree of causation for respective collision opponents

   – Other causes than negligence taken into the assessment such as objective factors affecting the impact of the damage, such as for example the type and size of the respective vehicles

THANK YOU!

FRANKFURT AM MAIN
Hamburger Allee 4 (WestendGate)
60486 Frankfurt am Main
T +49-69 97 98 85 0
F +49-69 97 98 85 85

MÜNCHEN
Oberanger 34–36
80331 München
T +49-89 388 08 0
F +49-89 388 08 101

HAMBURG
Große Elbstraße 36
22767 Hamburg
T +49-40 31 77 97 0
F +49-40 31 77 97 77

BERLIN
Kurfürstendamm 54/55
10707 Berlin
T +49-30 814 59 13 00
F +49-30 814 59 13 99

LEER
Am alten Handelshafen 3A
26789 Leer
T +49-491 960 71 0
F +49-491 960 71 20

DRESDEN
Am Brauhaus 1
01099 Dresden
T +49-351 866 59 0
F +49-351 866 59 59

COMITÉ MARITIME INTERNATIONAL

SEAWORTHINESS IMPLICATIONS
KIDNAP and RANSOM
P & I IMPLICATIONS

TIM HOWSE
Gard (UK) Ltd
CHARLES FERNANDEZ
Canopius Syndicate

Modern Technology, Cyber Crime and Marine Insurance

* Charles Fernandez
* Head of Marine Hull and Liability

canopius

Shipowner's Losses and Potential Policies

Losses Suffered	Potential Policies
• Physical Loss / Damage to Vessel	• H&M or War Policy
• Collision Liability	• ¾ H&M or War Policy and ¼ P&I Policy
• Loss of Hire	• H&M or War Loss of Hire Policy
• Ransom	• K&R Policy
• Liabilities	• P&I Policy

canopius

Damage to Vessel and ¾ Collision Liability

Assureds Claim	Potential Defences
• Recoverable under H&M policy under 6.1.1 “perils of the seas”	• Proximate cause of loss not perils of the seas but probably “piracy” or “seizure” or “person acting maliciously”
• Crew Negligence (Mandship only)	• Due Diligence Proviso • Unseaworthiness • Cl. 380
• Recoverable under the war policy as “piracy” or “seizure” or “person acting maliciously”	• Unseaworthiness • Cl. 380

canopius

Important Issues

1. What is the proximate cause of loss?
2. Can this be described as “Piracy” and / or “Seizure”?
3. Would this fall within the war peril of “person acting maliciously”?
4. Underwriters potential defences

*

canopius

Proximate Cause

- **What is the proximate cause of loss?**
  - Perils of the seas?
  - Crew Negligence?
  - Peril covered under the war policy?

- ***Causa proxima non remota spectatur***

- **Meaning of Proximate Cause**
  - Not proximate in time but efficiency
  - Effective or dominant cause

canopius

The evolution of piracy?

Past

Present

Future?

canopius

Piracy

* **Does the act of piracy have to be from a ship?**
  - Rule 8 of the Rule of Construction of the MIA states “the term pirates includes… rioters who attack the ship *from the shore*”.

* **Does there have to be a specific motive?**
  - Pirates act for their own gain or desire to cause damage
  - No political or ideological motives.

* **Does piracy have to involve force?**
  - Piracy is not committed by stealth.
  - There must be “force” or “threat of force”. *The Andreas Lemos (1982)*

canopius

Seizure

- **“Seizure seems to be a larger term than capture and goes beyond it, and may reasonably be interpreted to embrace every act of taking forcible possession either by lawful authority or by overpowering force.” Cory & Sons v Burr (1883).**
- **Not limited to action of a State.**
- **Was there “forcible possession” just prior to the collision or grounding?**
- **Was there “forcible possession” at the time of ransom demand?**

canopius

Person Acting Maliciously

- **Clause 1.5 of the Institute War clauses**
- **Covers loss or damage to the vessel caused by "… any terrorist or any person acting maliciously or from a political motive"**
- **Wide clause**

canopius

Insurers Potential Defences: Unseaworthiness

- **Three requirements**
  - Vessel unseaworthy
  - Privity of the assured
  - Loss attributable to the unseaworthiness

- **Were the vessels unseaworthy?**
  - Definition under the MIA: “A ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured”.
  - The ordinary, careful and prudent shipowner test. *McFadden Vs Blue Star Line (1905)*

canopius

Insurers Potential Defences: Unseaworthiness

- **Was there privity of the assured?**
  - Knowledge of the unseaworthiness
  - Privity includes “blind eye knowledge”
  - Privity has to be of the assured or their *alter ego*
  - Very difficult to prove

- **Was the loss attributable to the unseaworthiness?**
  - “Attributable to” NOT “proximately caused by”
  - Unseaworthiness only needs to be a remote cause.

canopius

Insurers Potential Defences: CL 380

* **Cyber Exclusion Clause**

  - "….in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

  - Reason for the Cyber Exclusion Clause

canopius

Cover for Ransom

- **Under the K&R Policy**
  - Bespoke wordings
  - Can cover “extortion” or “cyber extortion”
  - Seaworthiness defence
  - Generally no Cl 380

- **Under the War Policy**
  - Peril – “seizure” or “piracy” or “persons acting maliciously”
  - Potential General Average
  - Seaworthiness defence
  - Cl 380
  - Escape Clause

canopius

Conclusion

- Current legislation and policy wordings not designed for this scenario
- No authority on current facts
- Which policy responds will depend on the proximate cause
- Underwriters might have policy defences
- The insurance industry can provide cover for these scenarios

canopius

CYBERCRIME & MARINE INSURANCE

Tim Howse

Vice President, Gard (UK) Ltd.

9 November 2018

CYBERCRIME & MARINE INSURANCE
INTRODUCTION

- Background:
  - Software: all ships fitted with operational and navigational software supplied by Autonav Inc. (USA) which had malware (i.e. computer virus) installed via the Autonav Inc. technicians
  - Hardware: all ships' engine management control systems (EMCS) fitted with lookalike Brightspark chips preloaded by Black Hat with malware (i.e. computer virus)

- Ship specific issues:
  - Mandship: Black Hat took control of the navigation (bad firewall design combined with unauthorised computer gaming by crew) which gave control to the EMCS
  - Autoship: unclear whether Black Hat took control of navigation or just used the EMCS; cyber security of London Control Centre questioned
  - Tanker: Black Hat gained control of EMCS and navigation systems (questions over how)

CYBERCRIME & MARINE INSURANCE

SEAWORTHINESS – CARRIAGE OF GOODS (FOR EACH SHIP)

- Seaworthiness – Hague/Hague Visby Rules

"Article III

*1. The carrier shall be bound **before and at the beginning of the voyage** to exercise **due diligence** to:*

*(a) Make the ship **seaworthy**;*

"Article IV

*2. **Neither the carrier nor the ship shall be responsible for loss or damage arising or resulting from**:*

*(a) **Act, neglect, or default of the master, mariner**, pilot, or the servants of the carrier in the **navigation or in the management** of the ship. […] (c) **Perils**, dangers and accidents of the sea or other navigable waters. […] (e) **Act of war**. (f) **Act of public enemies**. […] (p) Latent defects not discoverable by due diligence. […] (q) **Any other cause arising without the actual fault or privity** of the carrier… but the **burden of proof** shall be on the person claiming the benefit of this exception …"*

CYBERCRIME & MARINE INSURANCE

SEAWORTHINESS – CARRIAGE OF GOODS (FOR EACH SHIP)

- Analysis of HVR Article III/1 & IV/2

  - **Mandship**: Black Hat took control after the voyage began (?), via the badly designed firewall and unauthorised crew computer activities; causative failure of due diligence before/at the beginning of voyage? If so, cannot rely on article IV/2(a) or any other defences under IV/2?

  - **Autoship**: was this the result of the malware – or control centre issue – unseaworthy yet unclear whether causative (negligence of Autonav technicians may amount to failure of due diligence by carrier) – unclear on whether article III/1 fulfilled – may not be able to rely on defences under IV/2?

  - **Tanker**: Black Hat gained control of EMCS and navigation systems (question how); uncertainty over causation – the burden rests with the carrier to prove the exercise of due diligence at the relevant time – if so can use article IV/2(a)?

CYBERCRIME & MARINE INSURANCE

SEAWORTHINESS – CARRIAGE OF GOODS (FOR EACH SHIP)

- HVR article IV/2(c), (e), (f), (p), (q) – other possible defences

  - Act of war – we don't know (may not be an action of a state)
  - Perils, dangers and accidents of the sea – unlikely (is this terrorism/cyber-attack?)
  - Act of public enemies – maybe
  - Latent defect – not really a "defect": this was deliberate (albeit maybe undiscoverable)
  - Any other cause arising without the actual fault or privity of the carrier – possibly

CYBERCRIME & MARINE INSURANCE

P&I IMPLICATIONS – CREW INJURY, CARGO DAMAGE, DELAY AND CHARTERPARTY CANCELLATION

*"**Rule 58: War risks***

*1 The Association **shall not cover** under a P&I entry liabilities, losses, costs or expenses … caused by: a war, … or any hostile act by or against a belligerent power, **or any act of terrorism** (provided that, in the event of any dispute as to **whether … an act constitutes …terrorism, the Association shall in its absolute discretion determine …[…]***

*2 The exclusion in Rule 58.1 above **shall not apply to** […] a demand made under*

i a guarantee [under] the Federal Maritime Commission under Section 2 of US Public Law 89-777, or

ii a certificate [under] the International Conventions on Civil Liability for Oil Pollution Damage 1969 or 1992 …, or

*iii an undertaking [to the IOPCF] 1992 in connection with the [STOPIA] (STOPIA), or, except where such liabilities, costs and expenses arise from or are caused by **an act of terrorism**, the Tanker Oil Pollution Indemnification Agreement as amended (TOPIA), or*

iv a certificate [under] the International Convention on Civil Liability for Bunker Oil Pollution Damage, 2001

v a certificate [under] the Nairobi International Convention on the Removal of Wrecks, 2007, or

vi a certificate under [under] Maritime Labour Convention […]"

CYBERCRIME & MARINE INSURANCE

P&I IMPLICATIONS – CREW INJURY, CARGO DAMAGE, DELAY AND CHARTERPARTY CANCELLATION

"Appendix I

2 War risks

The Association has arranged an additional war risk insurance for the benefit of its Members.

Scope of cover

1 The special war risk P&I insurance will cover P&I risks set out in Part II, Chapter 1, of the Rules for Ships, caused by war risks as described in Rule 58 of the Rules for Ships…subject to a minimum deductible of USD 50,000 any one event each Ship. Further, the ***cover includes liabilities arising from acts of terrorism as defined in the US Terrorism Risk Insurance Act 2002*** *as amended. …*

[…]

Limitation of cover

5 The cover for owners is limited to USD 500 million any one event each ***Ship in excess of the proper value of the entered Ship or any amounts recoverable under any other P&I war risks cover which the Member has arranged, whichever is greater****. The minimum excess is the proper value of the Ship determined in accordance with Rule 71.1(a) of the Rules for Ships or USD 100 million, whichever is the lesser."*

CYBERCRIME & MARINE INSURANCE

P&I IMPLICATIONS – CREW INJURY, CARGO DAMAGE, DELAY AND CHARTERPARTY CANCELLATION

"Appendix I

2 War risks

Bio chem and computer virus

*4 The Association **shall not be liable** for any losses…arising from:*

i any chemical, biological, bio-chemical or electromagnetic weapon;

*ii the use or operation, **as a means for inflicting harm, of any computer virus**;*

iii Clause 4 (ii) above will not operate to exclude losses (which would otherwise be covered under the terms of this policy) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

***However,** …covered through a **special pooling facility, covering the Member's liability in respect of**:*

*i damages, compensation or expenses in consequence of **personal injury to or illness or death of any seamen**; and*

*ii **for legal costs and expenses incurred solely for the purpose of avoiding or minimising any other P&I liability arising from a BioChem Risk**.*

*The limit of cover …is **USD 30 million per Ship** in the aggregate. […]."*

CYBERCRIME & MARINE INSURANCE

P&I IMPLICATIONS – CREW INJURY, CARGO DAMAGE, DELAY AND CHARTERPARTY CANCELLATION

Terrorism?

Generally no club clover (i.e. Gard Rule 58) but:

- War cover exits under additional insurances:
  - Covers acts of terrorism up to US$500m (above proper value/US$100m);
  - Excludes losses caused by computer virus used as a ***means of inflicting harm***;
  - Special pooling facility reinstates cover but only up to US$30m for crew injury plus sue and labour

War policy will most probably cover normal P&I type risks

CYBERCRIME & MARINE INSURANCE

SUMMARY AND CONCLUSIONS

- All three ships likely physically unseaworthy (not virus free)
  - Due diligence before/at the beginning of the voyage is the issue:
    - Probably a failure of due diligence on Mandship (firewall/unauthorised crew gaming)
    - Unclear for Autoship and Tanker (and London Control Centre) – further investigations
    - Mandship may struggle to rely on HVR defences;
    - Autoship/tanker may succeed on HVR defences subject to causation/further investigations
- Ultimately might be no standard P&I cover if this is ***act of terrorism*** within the war risk exclusion (i.e. Gard rule 58) but the club has discretion on whether to treat this as "terrorism"
- There would still be cover for liabilities to crew and in respect of legal costs/expenses to minimise P&I liabilities (carveout from the war risk exclusion filled by special pooling facility)
- Certified liabilities (i.e. Blue Card liabilities) covered (i.e. pollution/wreck removal)

CYBERCRIME & MARINE INSURANCE

SUMMARY AND CONCLUSIONS

- Other issues:
  - Limitation of liability (wreck removal and pollution)
  - Rights of recourse (product liability: negligence of Autonav Inc.)

- Regulatory Scoping Exercise:
  - HVR and YAR might usefully cover cyber events? CMI…
  - Convention on limitation in respect of cyber terrorism to tackle aggregation issue?
  - What about the possibility of breaking limits under any such convention?


THANK YOU….
WWW.GARD.NO

COMITÉ MARITIME INTERNATIONAL

COFFEE!

COMITÉ MARITIME INTERNATIONAL

CYBERSECURITY
ON SHORE and ON BOARD
LIMITATION of LIABILITY

PATRICK O'KEEFFE
AMC Solutions
JULIAN CLARK
Hill Dickinson LLP
BORIANA FARRAR
American Club

THE AMERICAN CLUB

CYBERSECURITY: THE NEW ENIGMA

THE PERSPECTIVE OF A P&I CLUB

Boriana Farrar

Vice President / Counsel (SCB,Inc.)
Business Development Director, North America

London, November 8-9,2018

P & I insurance

- IG P&I policies do not specifically identify cyber risks
- A cyber 'hostile act' or act of terrorism (a war risk) would be excluded from P&I cover
- FD & D Cover – may be coverage for legal costs & guidance if crime / dispute / loss directly involves an insured vessel

Regulatory Policies

- Alternative Security Program Plan holders now being asked to incorporate cyber into their next revision
- LNG/ CDC facilities will be required to include cyber in their next plans beginning (probably) next year.
- IMO has addressed cyber at Maritime Safety Committee level
- Revision/Draft to electronic Navigation and Vessel Inspection Circular NAV NVIC will includes cyber

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.

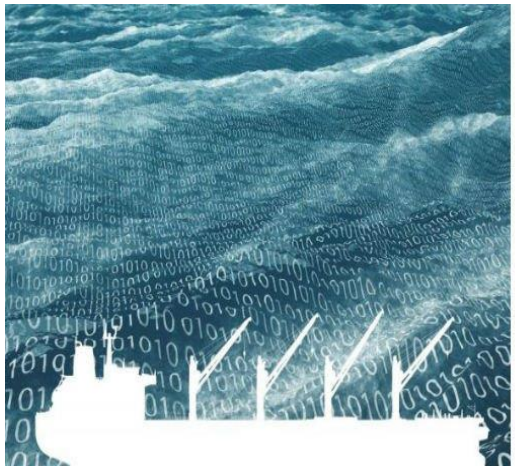
- The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (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.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

- **Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI**



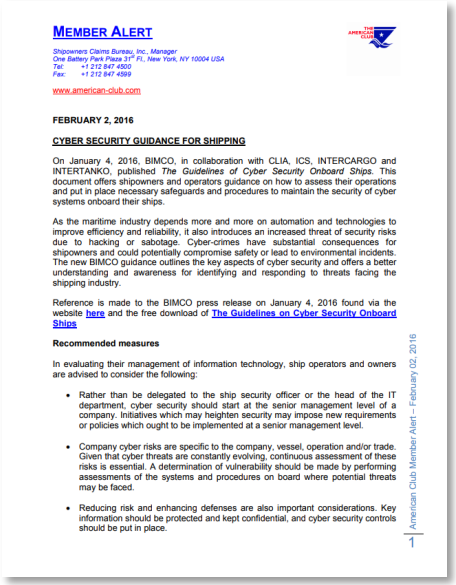
BIMCO


Cyber security approach
Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to and recover from cyber security incidents
Respond to and recover from cyber security incidents that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

American P&I Club

- Promoted by The American P & I Club to Members, with reminders of recommended measures
- Member Alert- American Club Cyber Security Guidance issued 2/2016:

http://www.american-club.com/files/files/MA_020216_Cyber_Security_Guidance_for_Shipping.pdf



MEMBER ALERT

Shipowners Claims Bureau, Inc., Manager
One Battery Park Plaza 31st Fl., New York, NY 10004 USA
Tel: +1 212 847 4500
Fax: +1 212 847 4599

www.american-club.com

FEBRUARY 2, 2016

CYBER SECURITY GUIDANCE FOR SHIPPING

On January 4, 2016, BIMCO, in collaboration with CLIA, ICS, INTERCARGO and INTERTANKO, published *The Guidelines of Cyber Security Onboard Ships*. This document offers shipowners and operators guidance on how to assess their operations and put in place necessary safeguards and procedures to maintain the security of cyber systems onboard their ships.

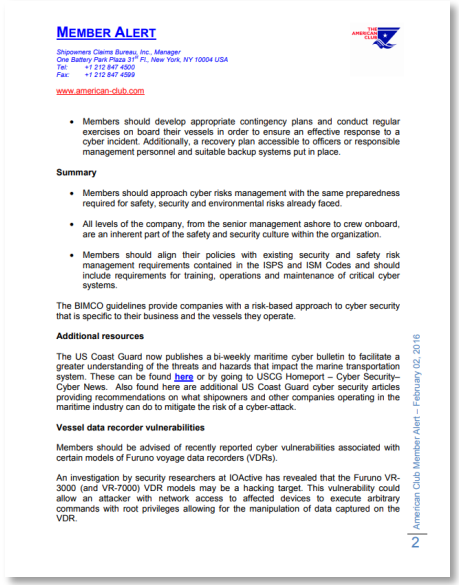
As the maritime industry depends more and more on automation and technologies to improve efficiency and reliability, it also introduces an increased threat of security risks due to hacking or sabotage. Cyber-crimes have substantial consequences for shipowners and could potentially compromise safety or lead to environmental incidents. The new BIMCO guidance outlines the key aspects of cyber security and offers a better understanding and awareness for identifying and responding to threats facing the shipping industry.

Reference is made to the BIMCO press release on January 4, 2016 found via the website here and the free download of The Guidelines on Cyber Security Onboard Ships

Recommended measures

In evaluating their management of information technology, ship operators and owners are advised to consider the following:

- Rather than be delegated to the ship security officer or the head of the IT department, cyber security should start at the senior management level of a company. Initiatives which may heighten security may impose new requirements or policies which ought to be implemented at a senior management level.
- Company cyber risks are specific to the company, vessel, operation and/or trade. Given that cyber threats are constantly evolving, continuous assessment of these risks is essential. A determination of vulnerability should be made by performing assessments of the systems and procedures on board where potential threats may be faced.
- Reducing risk and enhancing defenses are also important considerations. Key information should be protected and kept confidential, and cyber security controls should be put in place.



MEMBER ALERT

Shipowners Claims Bureau, Inc., Manager
One Battery Park Plaza 31st Fl., New York, NY 10004 USA
Tel: +1 212 847 4500
Fax: +1 212 847 4599

www.american-club.com

- Members should develop appropriate contingency plans and conduct regular exercises on board their vessels in order to ensure an effective response to a cyber incident. Additionally, a recovery plan accessible to officers or responsible management personnel and suitable backup systems put in place.

Summary

- Members should approach cyber risks management with the same preparedness required for safety, security and environmental risks already faced.
- All levels of the company, from the senior management ashore to crew onboard, are an inherent part of the safety and security culture within the organization.
- Members should align their policies with existing security and safety risk management requirements contained in the ISPS and ISM Codes and should include requirements for training, operations and maintenance of critical cyber systems.

The BIMCO guidelines provide companies with a risk-based approach to cyber security that is specific to their business and the vessels they operate.

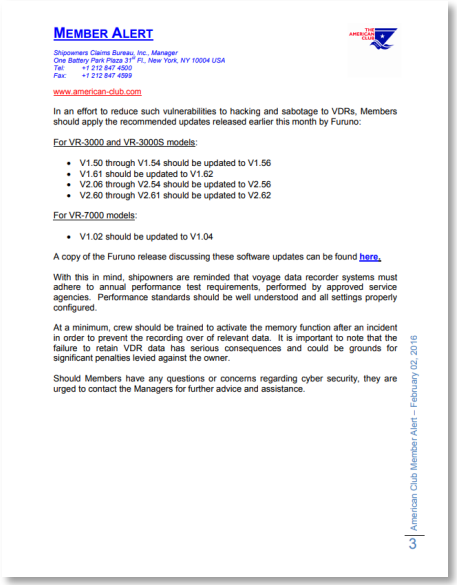
Additional resources

The US Coast Guard now publishes a bi-weekly maritime cyber bulletin to facilitate a greater understanding of the threats and hazards that impact the marine transportation system. These can be found here or by going to USCG Homeport – Cyber Security– Cyber News. Also found here are additional US Coast Guard cyber security articles providing recommendations on what shipowners and other companies operating in the maritime industry can do to mitigate the risk of a cyber-attack.

Vessel data recorder vulnerabilities

Members should be advised of recently reported cyber vulnerabilities associated with certain models of Furuno voyage data recorders (VDRs).

An investigation by security researchers at IOActive has revealed that the Furuno VR-3000 (and VR-7000) VDR models may be a hacking target. This vulnerability could allow an attacker with network access to affected devices to execute arbitrary commands with root privileges allowing for the manipulation of data captured on the VDR.



MEMBER ALERT

Shipowners Claims Bureau, Inc., Manager
One Battery Park Plaza 31st Fl., New York, NY 10004 USA
Tel: +1 212 847 4500
Fax: +1 212 847 4599

www.american-club.com

In an effort to reduce such vulnerabilities to hacking and sabotage to VDRs, Members should apply the recommended updates released earlier this month by Furuno:

For VR-3000 and VR-3000S models:

- V1.50 through V1.54 should be updated to V1.56
- V1.61 should be updated to V1.62
- V2.06 through V2.54 should be updated to V2.56
- V2.60 through V2.61 should be updated to V2.62

For VR-7000 models:

- V1.02 should be updated to V1.04

A copy of the Furuno release discussing these software updates can be found here.

With this in mind, shipowners are reminded that voyage data recorder systems must adhere to annual performance test requirements, performed by approved service agencies. Performance standards should be well understood and all settings properly configured.

At a minimum, crew should be trained to activate the memory function after an incident in order to prevent the recording over of relevant data. It is important to note that the failure to retain VDR data has serious consequences and could be grounds for significant penalties levied against the owner.

Should Members have any questions or concerns regarding cyber security, they are urged to contact the Managers for further advice and assistance.

A presentation by

HILL DICKINSON

HILL DICKINSON

In this session

- Is there a risk - can fiction become fact ?
- Seaworthiness continued.
- Limitation of liability.
- Application of the facts.

A warm up act for Patrick – fiction or fact

- Maersk not Petya
- 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 ?

Seaworthiness continued

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.

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?

Limitation of liability

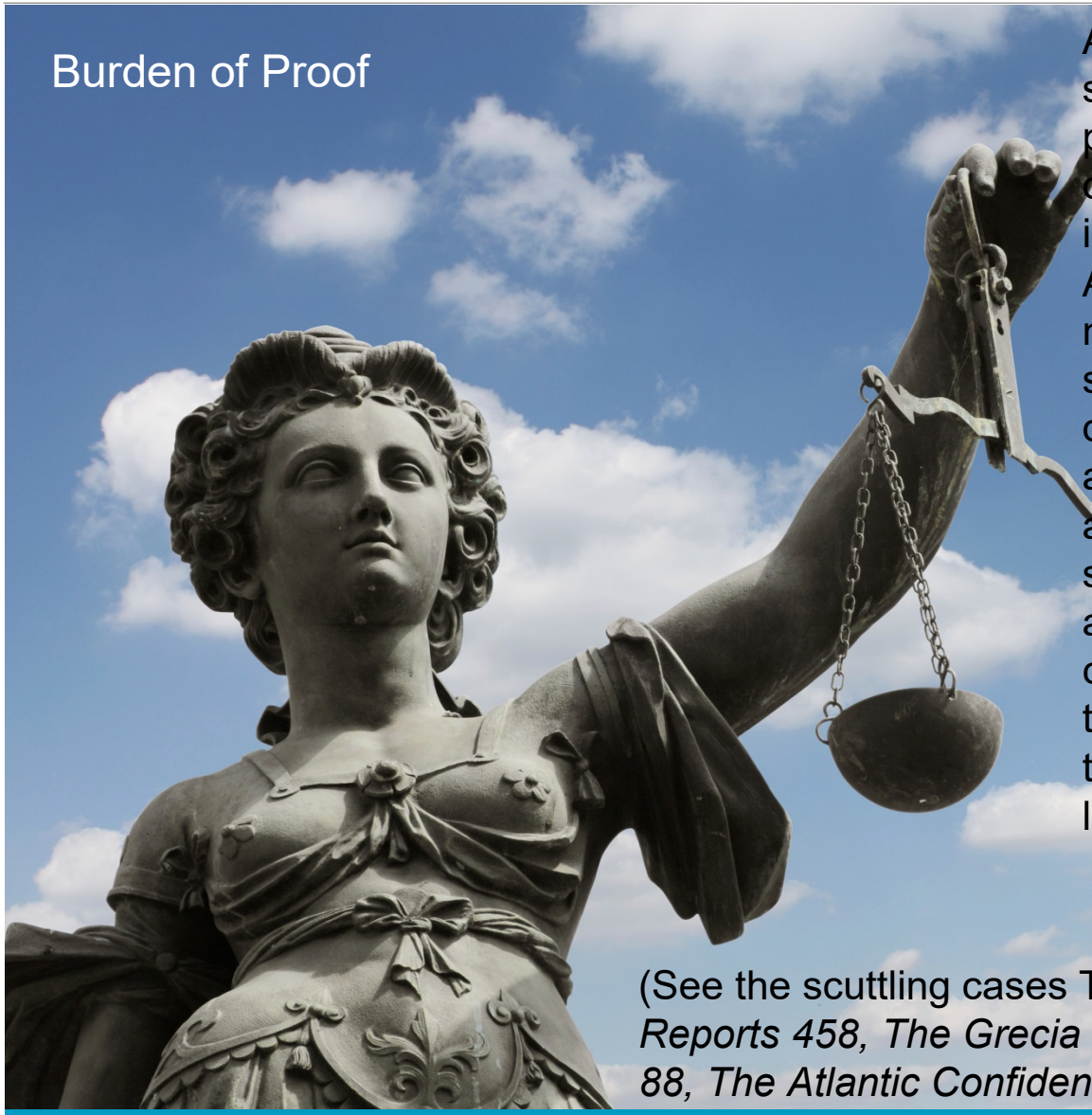
- Limitation of liability
  - 1957
  - 1976
  - 1996 Protocol
  - 2012

- 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

Application of the facts

- Original access gained due to an ability to break through the ships firewall protection
- Two junior officers playing computer games on personal laptops plugged into the mainframe in breach of the vessel standing instructions.
- Firewall protection design wholly inadequate.
- Complete inability to isolate separate networks.
- No evidence to suggest adequate cyber risk training

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.

HILL DICKINSON

Conclusion

- Dependant upon further investigation and evidence…
- Good chance to show causative unseaworthiness
- Significant risk of being able to establish a case based on recklessness in order to break limitation

A presentation by

HILL DICKINSON

CMI / IMO

The Challenging Convergence of Modern Technology, CYBERCRIME and Marine Insurance

---

Patrick O'Keeffe

Senior Research Associate
Institute for Security Policy
at Kiel University (ISPK)

Managing Director
AMC Solutions

@AskOKeeffe

www.patrickokeeffe.de

Who am I?

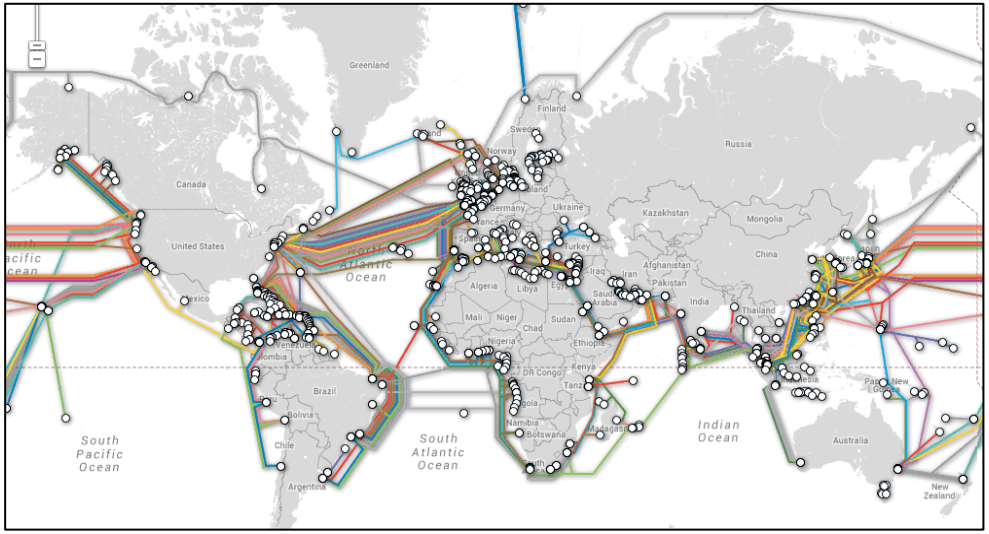
NATO OTAN

AMC
AEROSPACE MARITIME CYBER
Systems | Security | Strategy | Policy

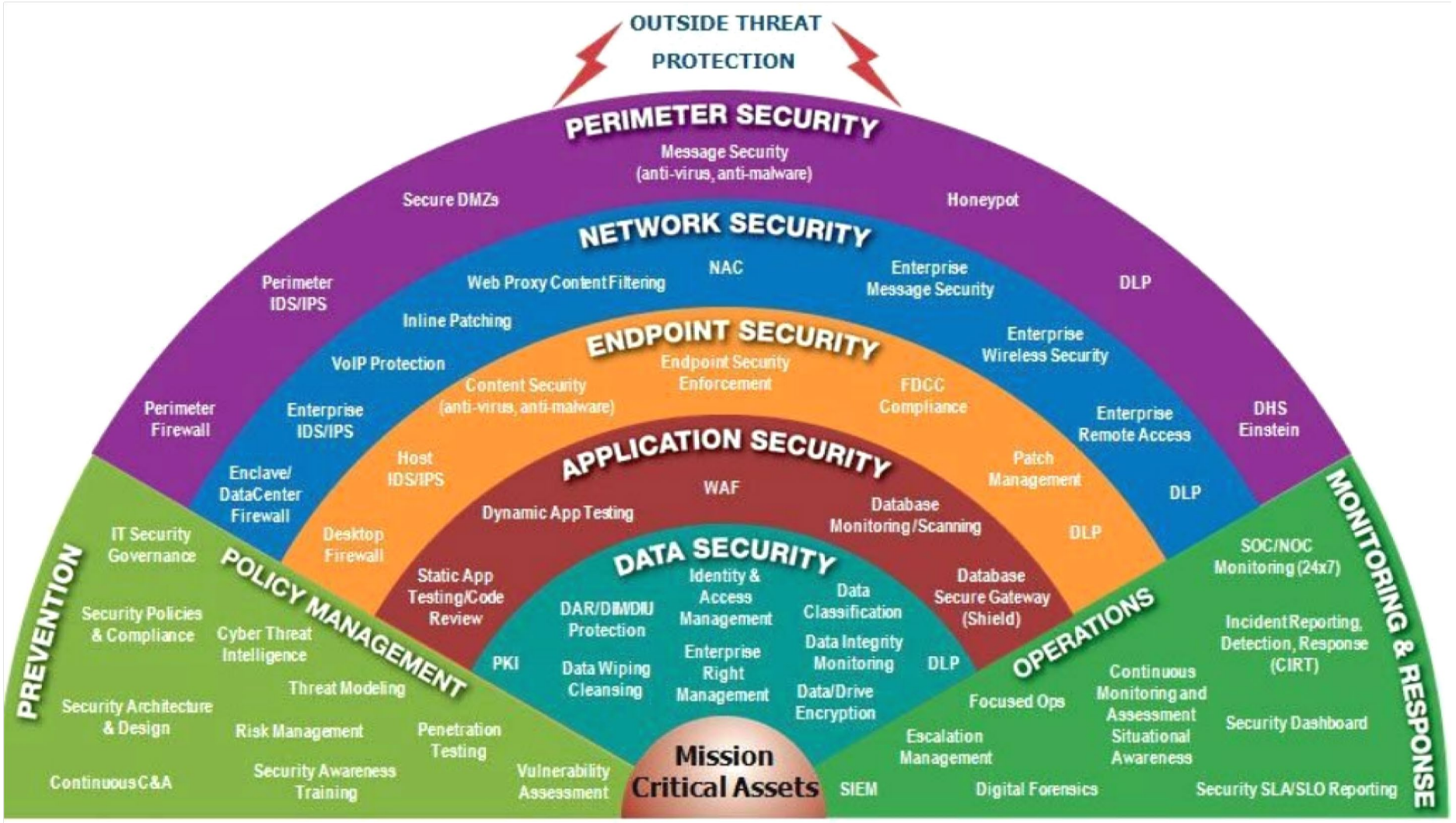
ISPK Institute for Security Policy Kiel University

CENTRE OF EXCELLENCE
COE
CSW
Operations in Confined and Shallow Waters

What is Cyberspace?



What is Cyber Security?



© PATRICK O'KEEFFE |
09 NOV 18

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

NotPetya:
10.000M USD Global Damage

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

A Ship is a Collection of:

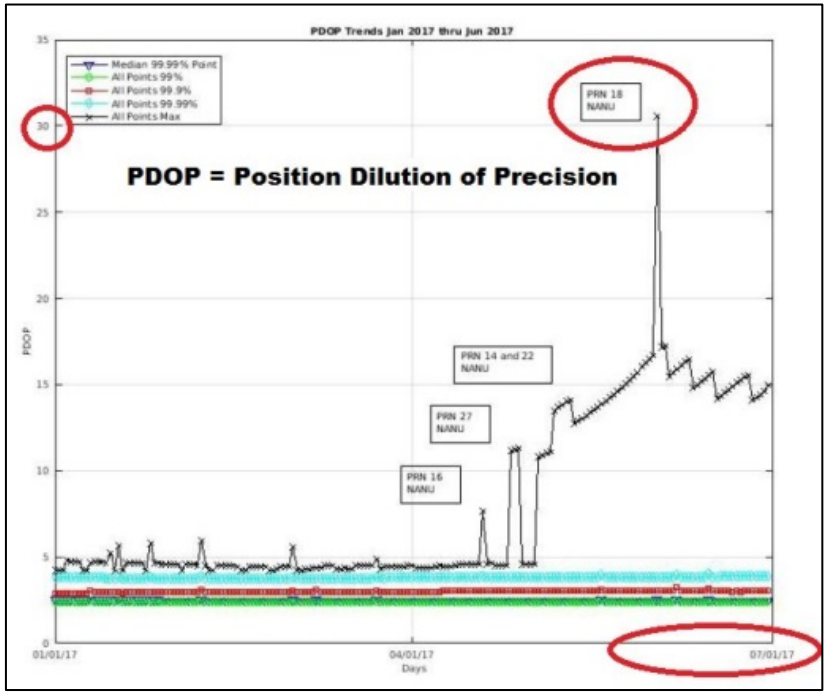
- **Outdated Systems**
- **Unpatched Systems**
- **Poor Trust Models**

And: Always Connected!

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

© PATRICK O'KEEFFE | 09 NOV 18

Who are the Enemies in Cyberspace?

Regierungs-einrichtungen	APT6/1.php, APT12/NumberedP., APT28/Sofacy, APT29/CozyBear, APT32/OceanLotus, Cadelle/Chafer, Callisto/DancingSal., CharmingKitten, Danti, DarkHotel, Dropping-Elephant, EmissaryPanda, Gamaredon, GazaCybergang, GothicPanda, Greenbug, Groundbait, HammerPanda, Infy, KeyBoy, Longhorn, LotusPanda, Machete, Mofang, Naikon/OverrideP., NanHaiShu, OilRig, Operati-on-Cleaver, Remsec/ProjectSauron, ScarletMimic, Shamoon, Snake, Suckfly, TidePool/Ke3chang, Transparent-Tribe, TropicTrooper/ PirateP., ViceroyTiger
Militär/ Rüstung	APT28/Sofacy, AridViper, Callisto/DancingSal., CharmingKitten, C-Major/PureStrike, Dropping-Elephant, Gamaredon, GazaCybergang, GothicPanda, HammerPanda, LotusPanda, Machete, Mofang, Naikon/OverrideP., OilRig, Operation-Cleaver, Remsec/ ProjectSauron, Snake
Energie	APT10, APT18/Wekby, APT29/CozyBear, CharmingKitten, ElectricPowder, EmissaryPanda, Greenbug, Kraken/Laziok, Longhorn, Machete, OnionDog, OperationCleaver, Sandworm, Shamoon, TropicTrooper/PirateP.
Opposition	Ahtapot, APT32/OceanLotus, Bookworm, FlyingDragon, Groundbait, Group5, Infy, Neodymium, Operation-Cleaver, Operation Manul, Promethium, ScarletMimic, Sima, StealthFalcon
Medien	APT28/Sofacy, APT32/OceanLotus, BugDrop, Callisto/DancingSal., DarkHotel, GazaCybergang, Groundbait, Infy, Operation Manul, Sandworm, ShroudedCrossbow, StealthFalcon, Tick
Finanzen	APT18/Wekby, APT29/CozyBear, EmissaryPanda, EquationGroup, GazaCybergang, HammerPanda, Longhorn, OilRig, Sandworm, Suckfly
Telko	APT18/Wekby, Codoso, EmissaryPanda, HammerPanda, Longhorn, Machete, OilRig, Remsec/ProjectSauron
NGO	APT29/CozyBear, Callisto/DancingSal., CharmingKitten, HammerPanda, Infy, NilePhish, Operation-Cleaver, RocketKitten
Universitäten	APT10/menuPass, BugDrop, Codoso, Greenbug, DarkHotel, Longhorn, RocketKitten
High-Tech	APT18/Wekby, CharmingKitten, Codoso, LEAD/Winnti, Tick
Transport/ Logistik	Cadelle/Chafer, OilRig, OnionDog, Remsec/ProjectSauron, Shamoon
Luft- und Raumfahrt	APT28, EmissaryPanda, HammerPanda, Greenbug, Longhorn
Gesundheit	APT10/menuPass, LEAD/Winnti, Suckfly
Kanzleien	APT29/CozyBear, Codoso, DeepPanda, NanHaiShu

Source: *„Die Lage der IT-Sicherheit in Deutschland 2017“*

Advanced Persistent Threat (APT) Lifecycle

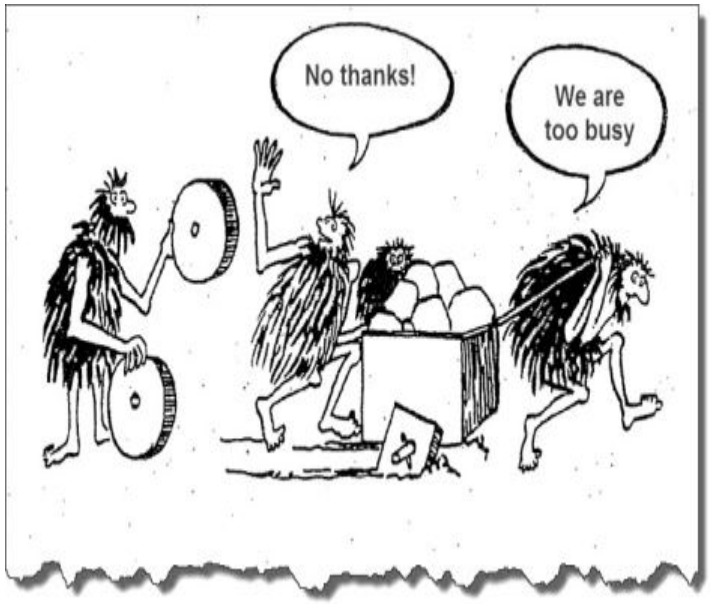
APT lifecycle

1. **Reconnaissance -** gathering information about the target
2. **Initial compromise** - exploit an entry point, gain foothold and establish outbound connection
3. **Maintaining access** - consolidating presence at entry point(s)
4. **Lateral movement** - compromise other host in the network; find data
5. **Data exfiltration** - extract data from internal network
6. **Cover tracks** - hide traces of malicious activities

What Can We Do?

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

© PATRICK O'KEEFFE |
09 NOV 18

COMITÉ MARITIME INTERNATIONAL

EXPOSURE
OF
CLASSIFICATION SOCIETIES

ANDERSON CHAPLOW
Lloyd's Register

A Classification Society perspective

CMI Joint International Sub-Committee Meeting
09 November 2018

Anderson Chaplow
Naval & Unmanned Lead Specialist
Lloyd's Register EMEA

Lloyd's Register

Introduction

- Safety critical control systems
- Cybersecurity
- Control system safety on autonomous ships

“The expansion of the scope of the traditional Classification remit to defend the safety of the ship and shipboard systems against a cyber threat”

Safety critical control systems

Principle:

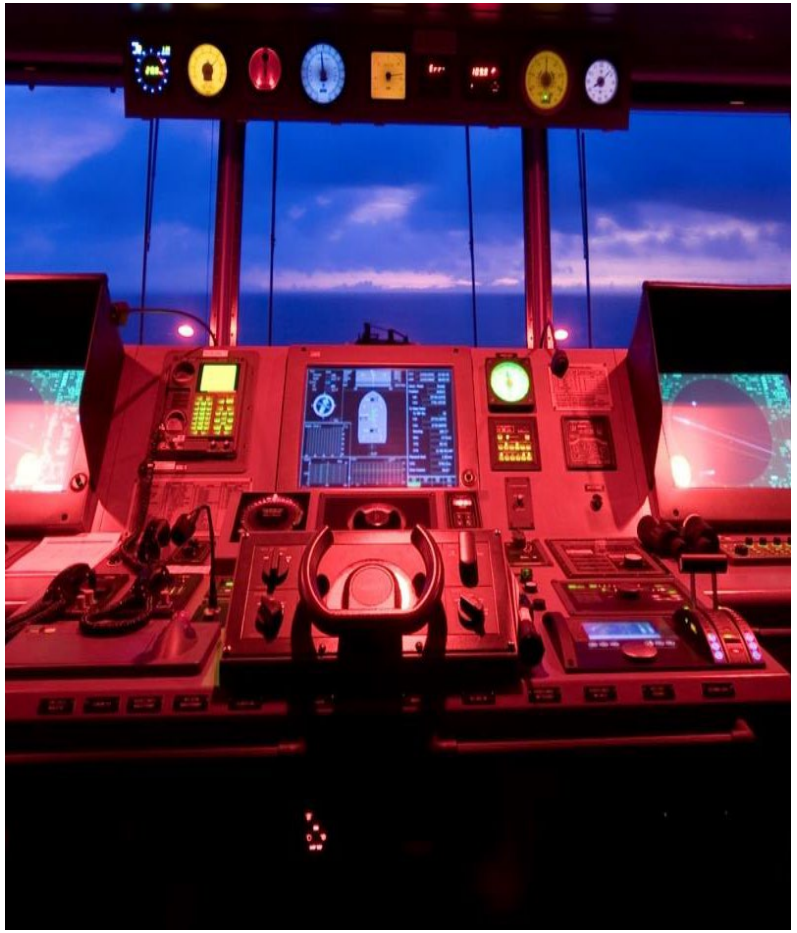
Failure of the control system is not to result in the loss of ability to provide essential services

Practise:

Existing requirements and audit-based tools for analysis of safety critical software

Conclusion:

Proven in a 'non-hostile' onboard cyber environment



Cybersecurity

Principle:

Provision of an appropriate level of access when, and where, required for safe operation

Practise:

Rapid development of requirements and services to protect access to critical 'Class' systems

Conclusion:

Expected to provide a degree of protection in a 'hostile' cyber environment but reliant on people

Control system safety on autonomous ships

Principle:

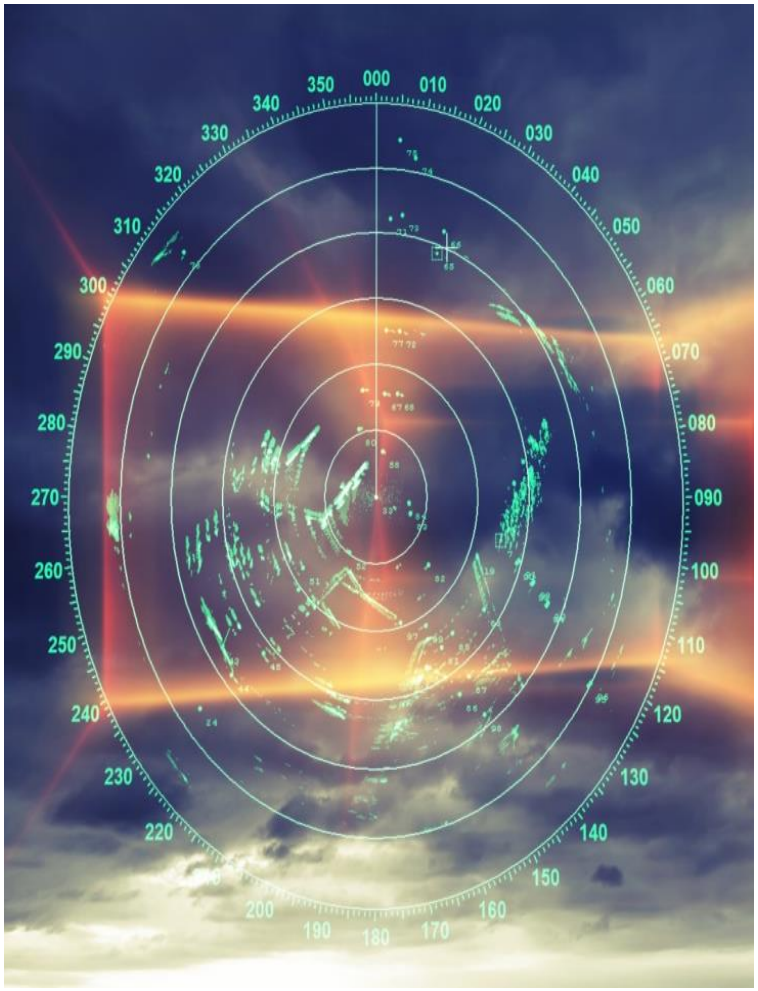
System of systems approach to whole ship safety based on standardised norms

Practise:

Controlled deployment of risk-based assurance on bounded pilot projects

Conclusion:

Reliant on development of standardised norms for navigation and sensor systems



Conclusions

Classification requirements are robust in respect of the means of assessing redundancy, diversity and performance of control systems

There is currently a gap in relation to cyber security but requirements are being developed and will soon be included within the Rules

The interactions between autonomous control systems and ship systems will expand the boundary of the traditional Classification remit and hence the possible exposure

Thank you

Please contact:

Anderson Chaplow

Lead Specialist – Naval Centre of Expertise
01275515500

anderson.chaplow@lr.org

COMITÉ MARITIME INTERNATIONAL

PRODUCT LIABILITY
LIABILITY OF SHIPYARDS
and
SOFTWARE INSTALLERS

ROBERT VEAL
University of Southampton

UNIVERSITY OF Southampton

Autonomous technology in shipping: an increased role for product / manufacturer liability?

CMI Joint International Sub-Committee Meeting
London, 2018

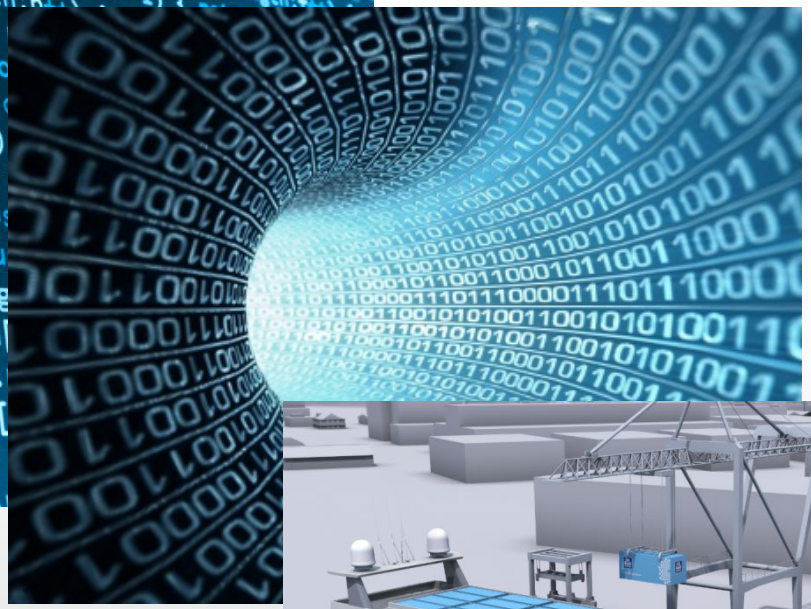
Robert Veal LL.B, LL.M
Lecturer in Law
University of Southampton

- **Third-party liability funnelled to shipowner**
  - Convention for the Unification of Certain Rules of Law with respect to Collisions between Vessels, 1910
  - International Convention on Civil Liability for Oil Pollution Damage, 1969
  - The International Convention on Civil Liability for Bunker Oil Pollution Damage 2001
  - Nairobi International Convention on the Removal of Wrecks 2007

- **Parallel actions against other parties?**

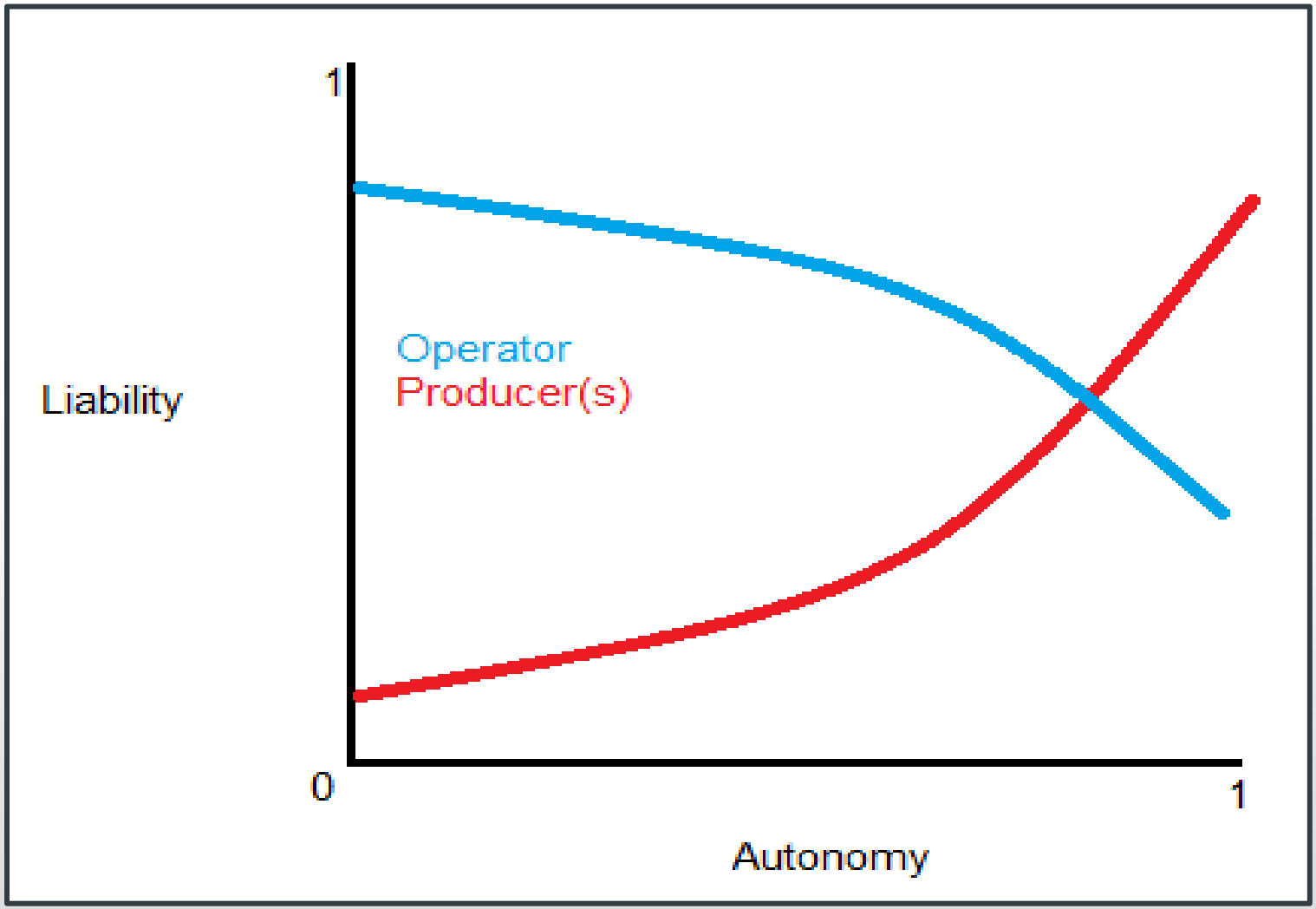
- **Large assumption of responsibility**
  - Maintenance, management and inspection (ISM, ISPS)
  - Vicarious liability (Crew)

Autonomous marine systems



- Hardware (sensors)
- Software
- Algorithms
- GPS / Communications
- Components thereof

A liability shift?



“Autoship“ and “Mandship“

Evidence shows that the MANDSHIP’s firewall protection design was wholly inadequate: the way it had been set up failed to isolate the various computer networks on board. Especially, the network used by the crew for comms was not properly isolated from the ship’s operating and navigation systems. This was a flaw in her design.

The Court hears that the unmanned AUTOSHIP was being intermittently monitored by suitably qualified mariners at its control centre in London. No alert was transmitted by the AUTOSHIP to the control centre as it came into close quarters with MANDSHIP. The AUTOSHIP’s Autonav software failed to respond and reduce speed and heading appropriately.

Product liability: sources of law

- Tort of negligence (England and Wales)
- EU Product Liability Directive 85/37 concerning liability for defective products

EU Directive 85/374

- Article 1
  - *The producer shall be liable for damage caused by a **defect** in his product.*
- Article 2
  - *For the purpose of this Directive 'product' **means all movables** … 'Product' includes **electricity**.*
    - Hardware
    - Spatial sensors
    - Software?
    - Algorithms?
    - *A service?*

EU Directive 85/374

- Article 9

- *For the purpose of Article 1 , 'damage' means :*
  *a) damage caused by **death** or by **personal injuries** ;*

  *b) damage to, or destruction of, any item of **property** other than the defective product itself, provided that the item of property :*

  - *(i) is of a type ordinarily intended for **private use** or consumption, and*
  - *(ii) was used by the injured person mainly for his own private use or consumption.*

EU Directive 85/374

- Article 4
- 1 . A product is defective when it does not **provide the safety which a person is entitled to expect**, taking **all circumstances** into account, including :
  - (a) the **presentation** of the product ;
  - (b) the **use** to which it could **reasonably** be expected that the product would be put ;
  - (c) the time when the product was put into circulation.

EU Directive 85/374

- Article 7
- The producer **shall not be liable** as a result of this Directive if he proves :
  - (d) that the defect is due to **compliance** of the product with **mandatory regulations** issued by the **public authorities** ; or
  - (e) that the state of **scientific and technical knowledge** at the time when he put the product into circulation was **not such as to enable the existence of the defect to be discovered** ; or
  - (f) in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.

The tort of negligence

562 HOUSE OF LORDS [1932]

[HOUSE OF LORDS.]

H. L. (Sc.)* 1932 May 26. M'ALISTER (or DONOGHUE) (Pauper) . Appellant;

AND

STEVENSON . . . . . Respondent.

Negligence—Liability of Manufacturer to ultimate Consumer—Article of Food—Defect likely to cause Injury to Health.

By Scots and English law alike the manufacturer of an article of food, medicine or the like, sold by him to a distributor in circumstances which prevent the distributor or the ultimate purchaser or from discovering by inspection any defect, is under a legal d ultimate purchaser or consumer to take reasonable care that th free from defect likely to cause injury to health:—

So *held*, by Lord Atkin, Lord Thankerton and Lord M Lord Buckmaster and Lord Tomlin dissenting.

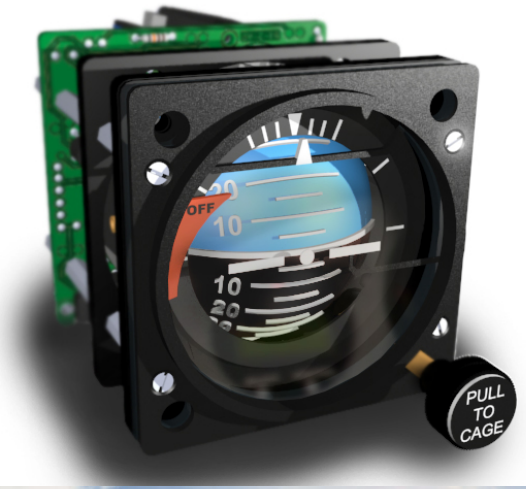
George v. *Skivington* (1869) L. R. 5 Ex. 1 approved.

Dicta of Brett M.R. in *Heaven* v. *Pender* (1883) 11 Q. 509–11 considered.

Mullen v. *Barr & Co., Ld.*, and *M'Gowan* v. *Barr & Co.*, S. C. 461 overruled.

The tort of negligence

- *Lambson Aviation v Empresa Aeronautica* [2001] All ER (D) 152.
  - Crash after failure of Artificial Horizon gyroscope
    - No duty owed
  - Important factors
    - Expectations of on-board crew
    - Compliance with CAA standards
      - "*considerable but not decisive weight*"
  - Causation?



A meaningful difference?

- Common salient factors:
    - Marketing, product warnings & management of expectations
    - Compliance with extant regulations / industry standards, testing procedures

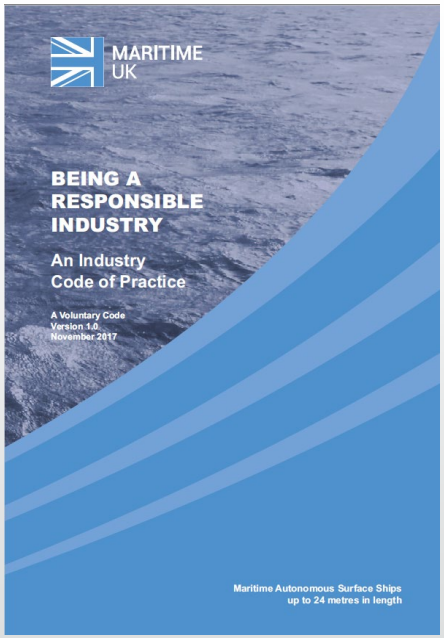
- J Stepleton, “Product Liability Reform – Real or Illusory? [1986] *Oxford Journal of Legal Studies*, pp.392-422.

“Reasonable” usage and supervision

- *Hindustan Steam Shipping Co Ltd v Siemens Bros & Co Ltd* [1955] 1 Lloyd's Rep. 167.
- “Intermediate inspection” defence prevails for *automation*
- Same expectation for *autonomy*?

Compliance with extant standards

- Important evidence but *not* dispositive (tort and Directive 85/374)
- No *uniform* standards for autonomous (marine) systems
  - National working groups
  - Class Societies
  - IMO
- Goal-based standards?
- **Insurance ?**



Concluding thoughts

- Advent of autonomy *may* place more onus on system producers
- Importance of consumer (and public) expectations of autonomy
- Causation rules probably determinative
- No international conflict of laws mechanism
- A question of policy and societal acceptance?

Thank you

- For more information, contact R.Veal@soton.ac.uk

COMITÉ MARITIME INTERNATIONAL

QUESTIONS

and

DISCUSSION

COMITÉ MARITIME INTERNATIONAL

THANK YOU

TO

ALL THE SPEAKERS

AND

TO IMO

COMITÉ MARITIME INTERNATIONAL

DRINK!!