Cyber Security Governance: The Case for a Cyber Code

Rory Hopcraft

About Me

Qualifications

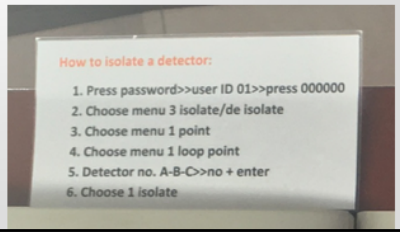
- BSc in Geography and Global Politics
- MSc in Geopolitics and Security
- CDT in Cyber Security

Research

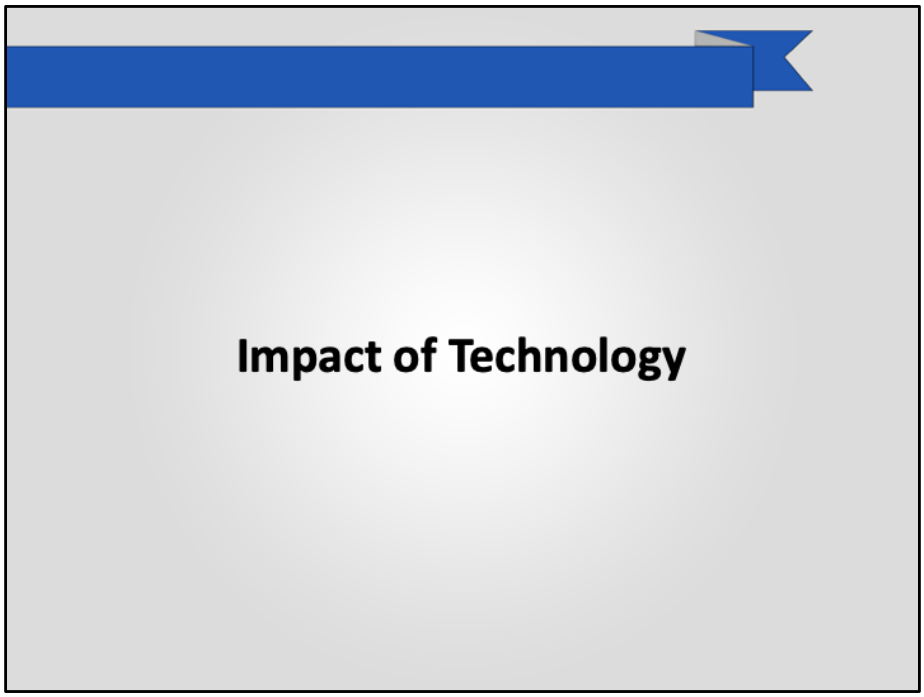
- "Regulatory Aspects of Maritime Cyber Security"
- Work with BIMCO and the IMO

Introduction

- Impact of Technology
- Regulatory Challenges
- Role of the Community
- Regulatory Instruments
- The Creation of a Cyber Code



Impact of Tech = Introduction
Challenges = problems with cyber regulation
Community = solution?
Codes etc = proof its possible
Cyber Code = what it actually entails (future)


Impact of Technology

- Past – containers
    - Massive impact on the way the industry works, from contracts to sending goods
- Present – Remote team
    - Smaller crews
    - Less skills onboard – outsourcing skills
    - Teams of non-maritime personnel upkeeping maritime systems
- Future – Autonomous??? (what ever this means)
    - How are these going to change the way the industry works?
    - What does autonomous mean? (unmanned engine rooms – MASS?)
    - Autonomous is just one of the possible futures

- Not a unique occurrence - similar discussion happening over alternative fuels
    - Seen the change from sail to steam to diesel
    - Help to ease the change and regulate that process

Traditionally the maritime was seen as:

- Ports – a place that allowed goods to be transferred from sea to land
- Crews – safety of the crew is always paramount to discussions – social media
- Ships – means to an ends – fastest most efficient way to transport goods from one place to another

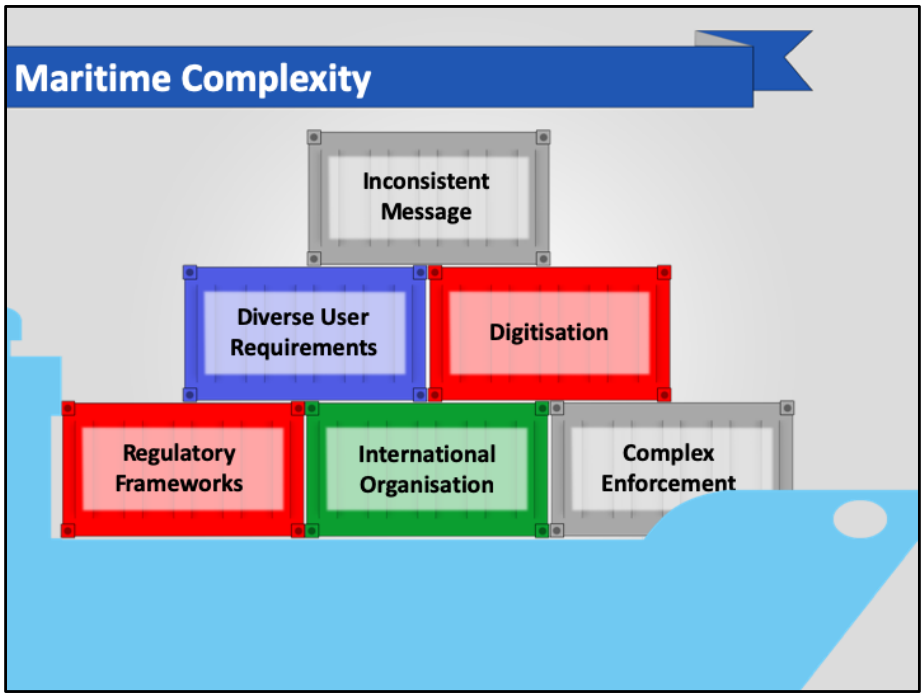
Technology has changed that:

- Users – from passengers to crew to office personnel all now connected to maritime cyber infrastructure – wider service teams
- Technology – more reliant upon it – numerous vendors – different systems layouts
- Satellites – GMDSS – communication – remote access etc – space always been part of of the discussion with IMSO etc but reliance is greater
- Enterprise systems – shared information platforms – HR systems – digital contracts (Maersk Example)
- Onward travel of goods – just in time principle – blockage of these cause problems for maritime (easer as digitally connected) = Port Antwerp example.

Secure the product supply chain

- Maritime no longer isolated


Regulatory Challenges



GENERAL CHALLENGES for Maritime Regulation

Regulatory Frameworks – UNCLOS, Codes and Conventions

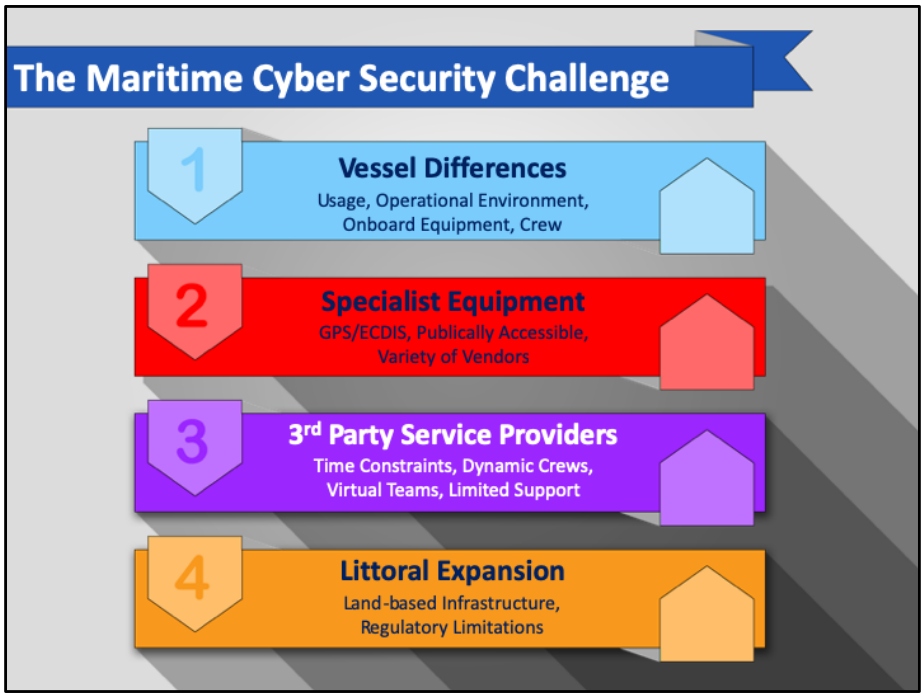
International Organisation's – IMO, shipping companies, think tanks, regional organisation (regional fishing organisations)

Complex Enforcement – IMO lacks enforcement capability – reliant upon member states, Classification Societies, Insurers

Digitisation – UNEVEN - Broad range of systems from navigation to automation – land infrastructure included

Diverse Requirements – Industry includes – fishing, cruise, tanker, offshore platforms, containers – PEOPLE are also included not just machines – safety is pinnacle in maritime

Inconsistent message - "Industry Expertise" not accurate and normally financially motivated – uncertainty suits them



Vessel Differences

- - fishing, cruise, tanker, offshore platforms, containers
- - short/long time at sea, Polar waters, storms, platforms completely different to ship
- - every vessel is unique – retrofitting of old with new – lifespan of vessel = 25+

Specialist Equipment

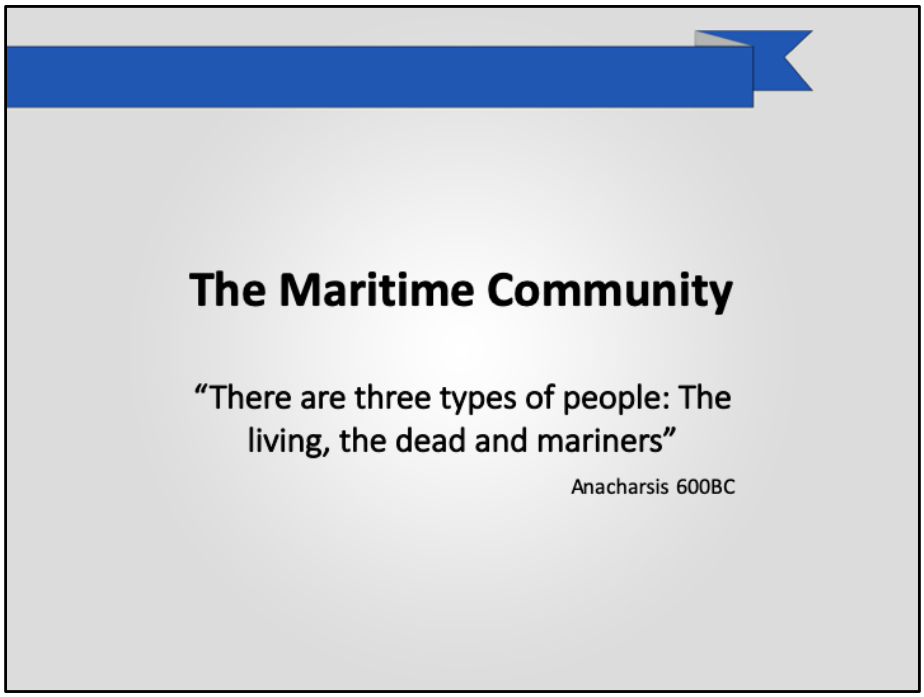
- - ECDIS, GPS – proprietary systems
- - IMO sets standards but up to vendor how these are met – not always compatible
- - Distress alerts must be publically available – GPS too
- - crew unable to maintain specialist equipment
- - differs vessel to vessel – crew maybe unsure of some of the systems
    - - work with a standard mode is being completed to give a generic looking interface

3rd Party Providers

- - Limited time for contractors to update/support/fix issues – limited to port time which is reducing.
- - Crew patterns change – training is unable to occur
- - reliant on so many different people for software
    - - vendor
    - - service provider
    - - shipping company
- - Limited physical access for support
- - Low-bandwidth connection

Littoral Expansion

- - linkage of land and sea infrastructure – not included in discussion increase in reliance
- - UNCLOS not include land – reliant on sovereign state



Grotius Freedom of the seas
Always been seen as a free and open expanse

"There are three types of people: The living, the dead and mariners"

- Escalation of security measures
    - Includes where states form alliances with others to address the increased security dilemma

- 2008 UN Secretary-Generals Report
    - A secure maritime space is a safer one
    - all states benefit from this.
    - all states responsible for addressing maritime safety and security threats

- UNCLOS - “common heritage of mankind, the exploitation and exploration of which shall be carried out for the benefit of mankind as a whole…”

- NGOs = ideologically driven not politically driven – means broader threats included in the security agenda (crime, drugs, piracy)

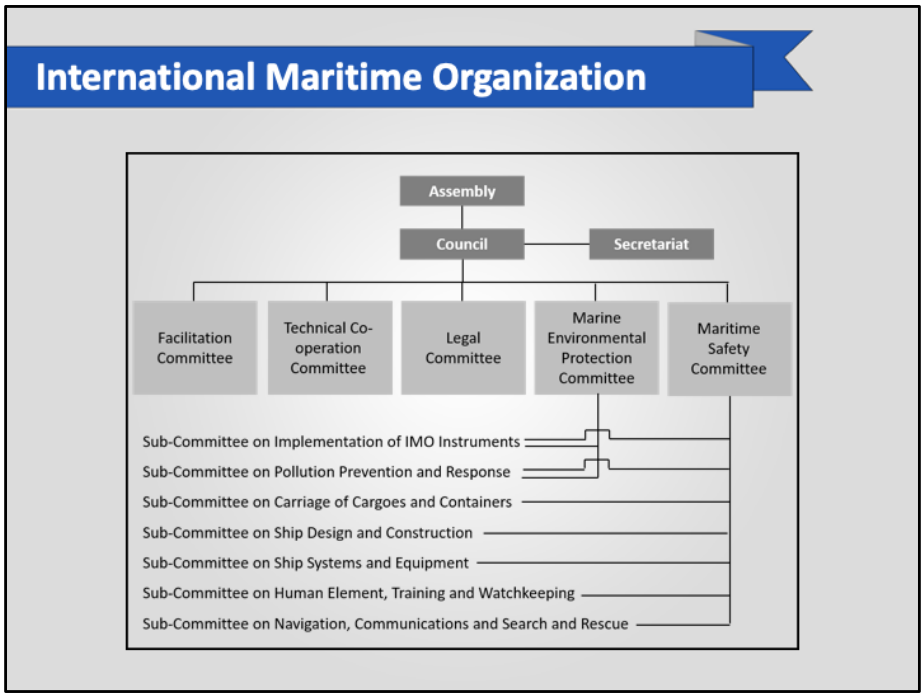
- **International Ship and Port Facility Security Code**
    - Reiterates responsibility of non-state in security
    - Owners/operators have to complete security plans
    - Plans assessed by other non-states on behalf of the state

- **UN Sustainable Development Goals**
    - world's best plan to build a better world for people and our planet by 2030
    - illustrate the broadening mandate of these supranational security collectives to include more than just security
    - Goal 14 – *Life Below Water* is central to the IMO's work - responsible to ensure all its members adhere to the goals – includes Non-State

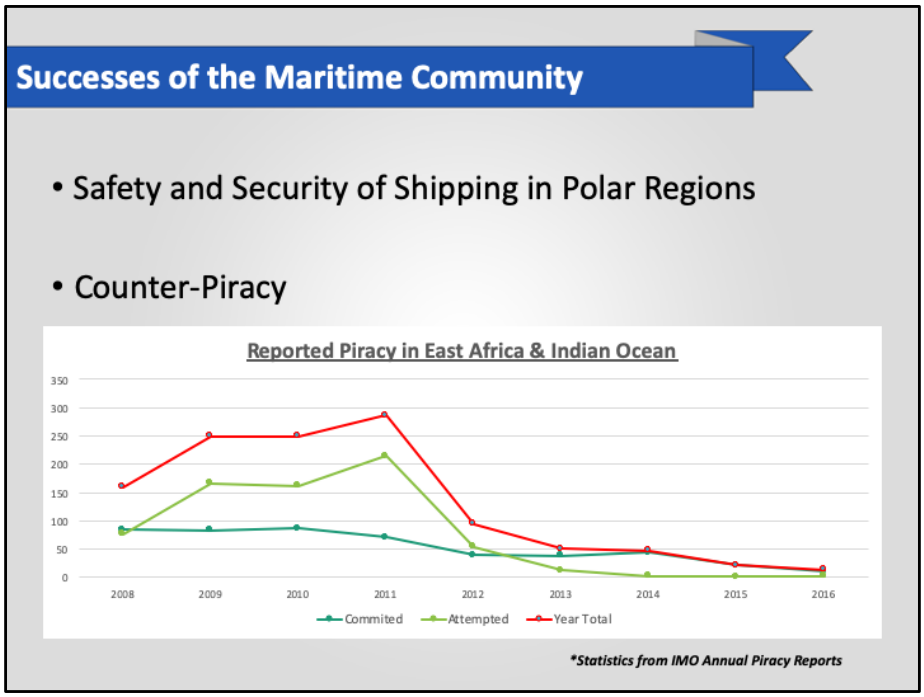
- Set up under UNCLOS to be the responsible organization for regulation

- Even the wording = community = OUR heritage
- Mission statement
  - Promote safe, secure, environmentally sounds, efficient and sustainable shipping through cooperation

- **Membership** = public/private
  - 174 member states
  - 81 NGOs
  - 64 IGOs
- Huge knowledge base



- **Structure**
  - Councils have specialties
  - Working groups take discussion further
- All members of maritime community are represented – through shipping associations etc
- Communities within communities
- Highlights the importance of those on the frontline!



Polar Regions

- Work of the Arctic Council generates policy-relevant knowledge of the region – environmental protection
- The Arctic Coastal States created agreements on commercial fishing in the region - sustainability
- The IMO through the Polar Code consider – shipping

Piracy

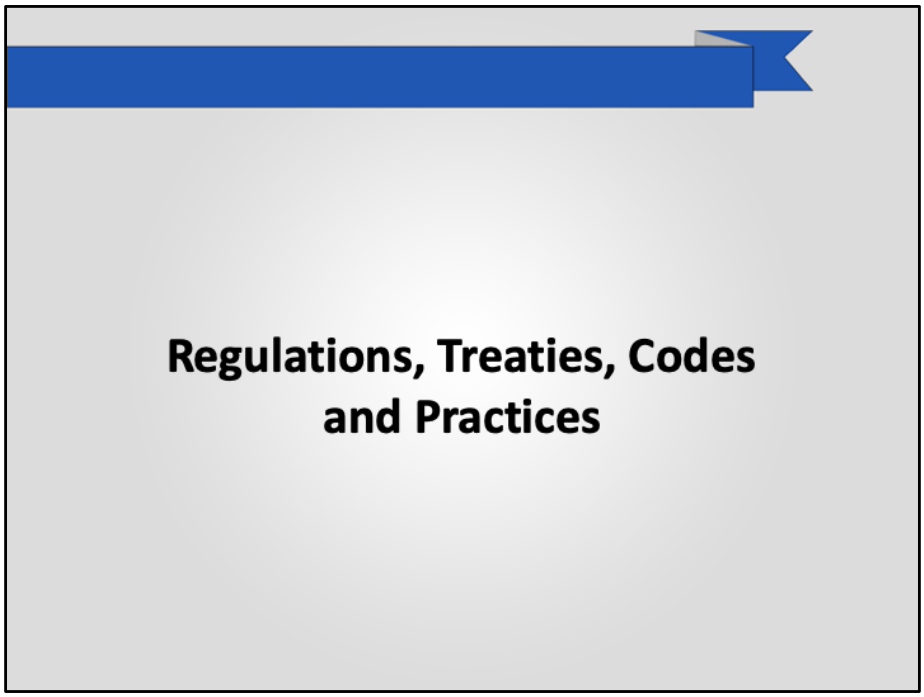
- International Maritime Bureau – Piracy reporting Centre = private information sharing
- Regional Cooperation Agreement on Combating Piracy and Armed Robbery against shops in Asia (ReCAAP) = government level sharing
- Singapore's Information Fusion Centre – Regional expertise on the fusion of information for the wider community

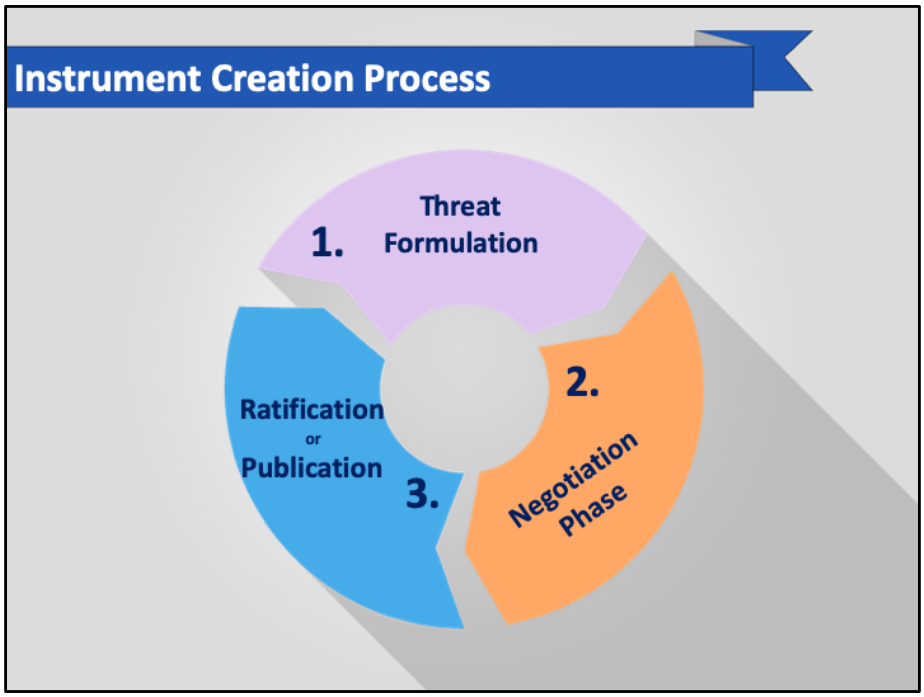
Djibouti Code of conduct – from international to regional capacity

- 2009
- Regional capability building
- Multi-lateral, multidiscipline security and facilitation committees
- If piracy occurs in state territory so hide behind sovereignty
- Complex geographical layout

- Information sharing of the region overcome some of the difficulties

NATO – Operation Ocean Shield


Regulations, Treaties, Codes
and Practices


Instrument Creation Process
1.
Threat Formulation
2.
Negotiation Phase
3.
Ratification
or
Publication

- Conventions
  - SOLAS, MARPOL
  - Large documents form the basis of all IMO regulations
  - Several parts (mandatory and voluntary)
  - Members MUST agree contents of conventions therefore act as treaties

- Circulars
  - Guidance from the IMO to clarify regulations
  - Not legally binding – some members may make them so

- Codes
  - Contain additional details not within a Convention
    - LSA Code, ISPS and ISM Codes – SOLAS
  - More of this in a minute

Traditionally a single ship event causes a regulatory change

- Titanic – SOLAS
- Deepwater Horizon – MarPol
- USS Cole
- MV Explorer

Event raises awareness of a set of risks – this publicity allows traction in regulatory discussions – prevent event occurring again

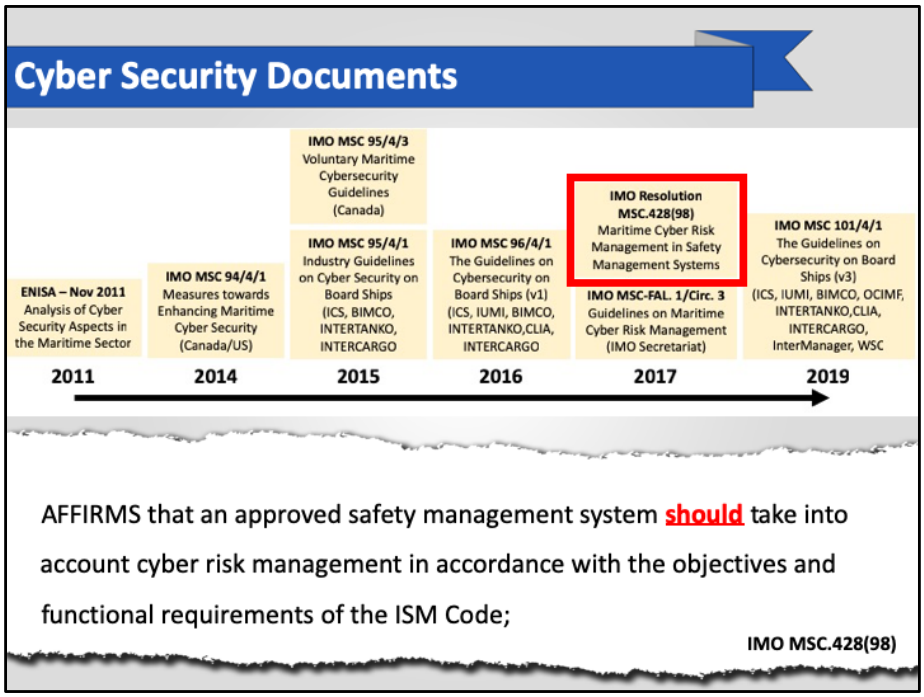
REACTIVE

SPEED 2 also not a good option

- Maersk
  - Not a deliberate attack – collateral damage to attack on Ukraine tax system
  - Far reaching consequences
  - Other companies (non-maritime) impact
- Russia
  - Black Sea, 2017
  - Putin's Summer House – stops GPS guided missiles
  - Vessel spoofed to airport

- Balance of cost over benefit


Maritime Cyber Security
Governance



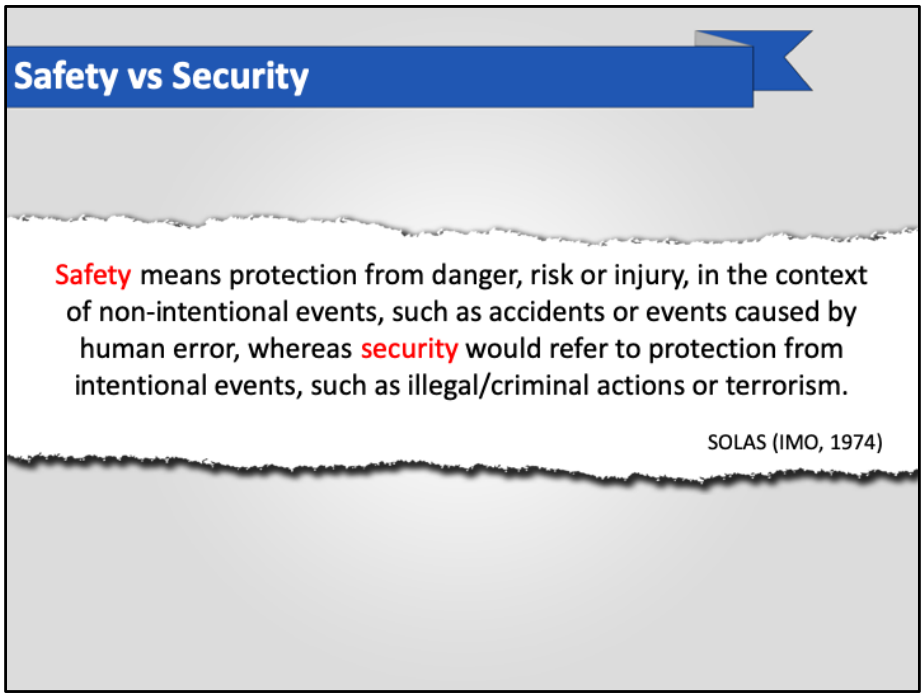
- Cyber Risk Management
    - Cyber security – to ridged – management suggests a journey and fluidity

- These risk assessments will increase the understanding of of cyber risk within the community
    - Negotiation phase…
    - Currently few actually report cyber incidents as insurance will not cover deliberate attacks
    - Not going to claim it was cyber if it means they wont get a pay out

    - As part of the SMS the assessments will form part of the Document of Compliance which can be checked by Port State Control

Cyber Risk Management Approaches

- IMO MSC.428(98)
- European Union (NIS Directive)
- Danish Maritime Authority
- IACS 12 steps
- BIMCO guidelines

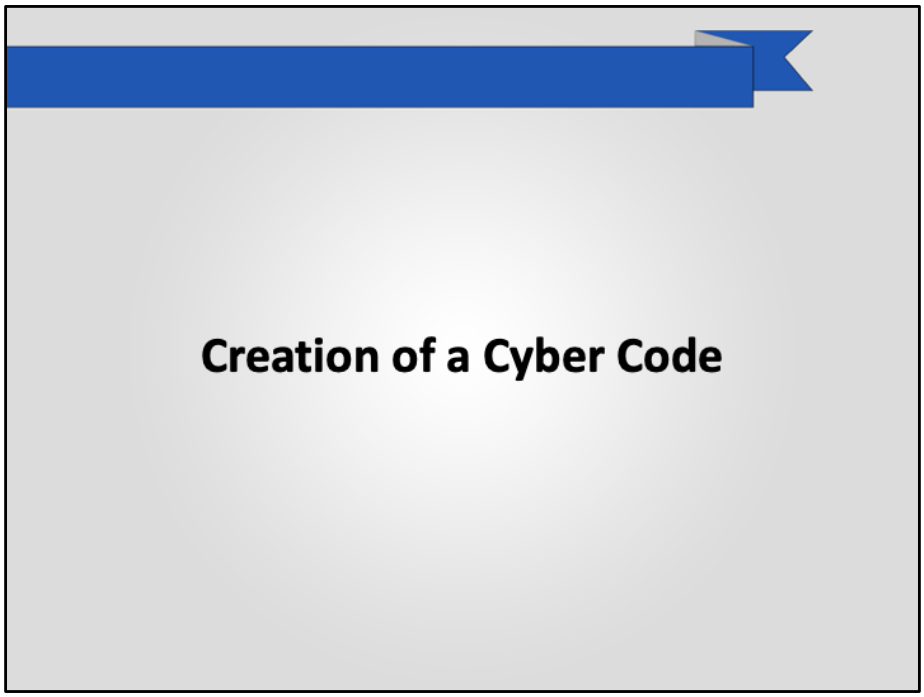


- DRAWBACK OF the ISM
- Cyber Risk Management not Cyber Security
    - Cyber security – to ridged – safety management suggests a journey and fluidity

- Becomes an important balance between cost and benefit!
- Focus on safety means there is little attention paid to deliberate cyber attacks…

- Example:
    - During berthing an on-shore engineer installed a patch remotely for engine room ventilation system
    - System rebooted shutting off the ventilation to the engine room (no oxygen being pumped in)
    - With engines running they used the remaining oxygen up in the space
    - With ship personnel in the space this could have had serious consequences
    - THIS WAS SAFETY as unintentional – same situation except deliberate attack with same consequences = Security threat.
- the ISM Code outlines that the company should identify equipment and technical systems the sudden operational failure of which may result in hazardous situations

Current State of Affairs


Creation of a Cyber Code

Legally binding treaties take a long time to create and implement – also mandatory requirements have more resistance to ratification

Overcome System Complexities

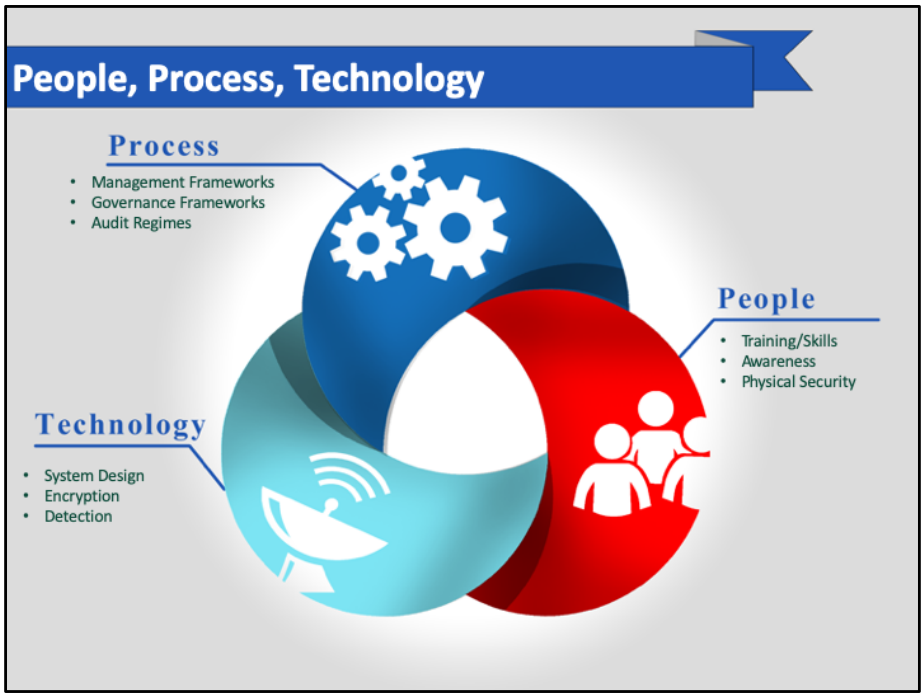
- One document – update, monitor, enforce
    - Modernise regulations as new tech/process appear – new 2018 e-waste IMO
- Harmonise standards – variety of systems with own requirements – easy to draw attention to them
- Harmonise other standards like NIST framework

Enable Enforcement

- Highlight responsibilities for enforcement
- Flags and Classifications are involved in discussions so develop enforcement with regulations
- Cyber Code would make things mandatory under international law – UNCLOS or SOLAS
- ISM/ISPS cyber risk assessments – starting point of having something to enforce

Overcome Sovereign Resistance

- Mandatory
    - Create a minimum level of compliance/ security
- Voluntary
    - Allows states to enact the less intrusive to sovereignty and comply
    - Allows those with reservations to allow code to enter into force



HOW CAN REGULATION APPROACH THE PROBLEM

Cyber Resilience gives us three pillars of cyber security – useful for regulatory discussions

- Process – already IMO Codes that outline certain processes and practices – ISM and ISPS do this
- People - Seafarers' Training Certification and Watchkeeping
- Technology – MarPol and NOx guidelines

IMO good at thinking about risks in this way – need to approach cyber in the same way…

- What process need to be in place to ensure vulnerabilities are not there?
    - Patch regimes
    - Update management – remote update vessel lost propulsion during berthing
    - What process are needed to verify this occurs
- People always seen as the weakest link - how do you strengthen this?
    - What training – stop removing all skills
    - Keep traditional skills like the manual compass
    - New skills of recognizing when information is wrong.

    - Raise awareness of the threats etc and provide support to overcome them – connectivity and the cost of SIM cards in ports etc.
- Technology
    - What makes a secure maritime system
    - How can these be updated – stop legacy systems
    - Firewalls etc
    - Physical security and access controls

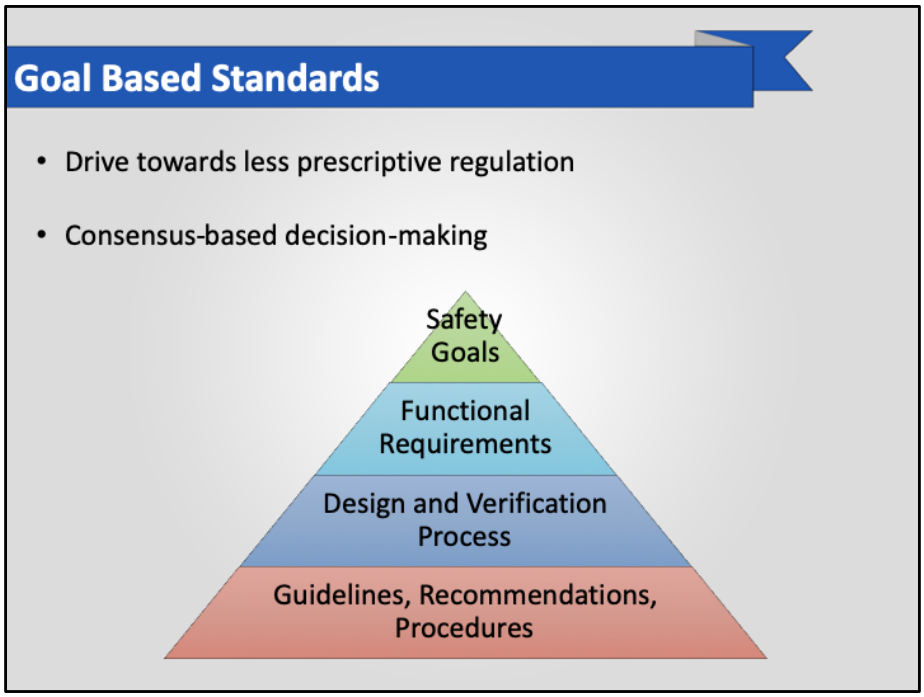
Polar Code – an Example?

CHAPTER 2 – POLAR WATER OPERATIONAL MANUAL (PWOM)

The goal of this chapter is to provide the owner, operator, master and crew with sufficient information regarding the ship's operational capabilities and limitations in order to support their decision-making process.

2.2.5 The Manual shall include or refer to specific procedures to be followed in the event that conditions are encountered which exceed the ship's specific capabilities and limitations in paragraph 2.2.2.

MEPC 68/21/Add.1 Annex 10



- Provide a basic safety/security standard – allow members to achieve this how they see fit
    - Application is appropriate to the ship, company, state, and regional demands (e.g. India runs on XP, or single ship company vs Maersk)

Conclusions

- Cyber Security is about more than just the maritime
- The Community is key to strong regulation
- Current regulation is the starting point
- Could a Cyber Code be the future?

Thank you for Listening

rory.hopcraft.2014@live.rhul.ac.uk

ROYAL HOLLOWAY UNIVERSITY OF LONDON

EPSRC Engineering and Physical Sciences Research Council

GEOPOLITICS & SECURITY

- Community needed for cybersecurity regulation
  - Firstly to understand the threat
  - Secondly – create the regulation
  - Thirdly – enforce the regulation