APPG ON CYBER SECURITY MEETING MINUTES 7th November 2022

Title: The meeting heard from three maritime sector experts in cyber security about the threats and challenges faced by the global maritime sector, which threatens the UK sector too and maritime domain and how these are being dealt with.

1. **Chairman's welcome** – Chair welcomed the three speakers and introduced them to the meeting.
2. **Present:** Chair – Simon Fell MP, Baroness Neville Jones
3. **Apologies:** Lord Arbuthnot of Edrom, Lord Mackenzie of Framwellgate, Rt Hon Sir George Howarth MP
4. **Speakers**:
   1. Andy Powell, CISO Maersk. Andy Powell is Chief Information Security Officer (CISO) at A P Moller- Maersk.

   Proliferating threat and support is needed. We have seen a 400% increase in weekly Cyber events. Significant issue for all the big carriers.
   Criminals, esp. Russian based ones, are working hard to improve their capabilities. Cyber weapons are shared and highly advanced. Supply chain exacerbates this. The increase inter connectedness of the supply chain has made matters worse. If one is hit, we are all hit. In South Africa, the Port Operating Authority was down for 3 weeks which costs millions of dollars. All in this together.

   Skills is an issue as we always need people. Technology, esp. AI is changing matters. Climate extremists are also a threat, not just cyber criminals. Also face recession which means less freight and cyber security may well be a victim of cost saving for many of the smaller carriers.

   Key things that we see is greater co-operation, works well with fellow Western CISOs. Tend not to share as much with Eastern CISOs. Need to build on that, but beware threats from China.

   Action is needed beyond just defending ourselves, need policing on an international basis. We need to cut off the funding for cyber criminals and their ability to develop software. 90% of trade goes by sea so need to do something.

   2. Rory Hopcroft, Research Fellow at the University of Plymouth.

   Slide 2 – sets the scene. Very basic cyber hygiene: has seen passwords laminated and stuck to control panels so anyone can read them.
   Slide 3 – visual representation showing how skills break down in an organisation. This includes shore side schemes. Management needs to understand the risk level and how

to mitigate this. Maersk handled their attack and gave people confidence that they knew how to handle it. Communication to the Media, Stakeholders etc. needs to be good and clear.
Slide 4 – found a vulnerability in a container vessel steerage system. Social engineering attack that could have been mitigated easily. The slide shows New York and how getting a ship stuck could cause havoc (cf. Suez).
Slide 5 - Who is involved in this kind of incident: crew, Port Authority, Ship owner etc. There are many stakeholders involved in an incident. Need to understand how these different elements work together. There is a lot of generic training out there, needs more cyber security training especially for those who may not touch IT onboard ship. An holistic approach to training is required to pull upon all the various stakeholders to ensure the effective management of cyber risk.
Slide 6 – shows the capabilities available in Plymouth. Safer to get it wrong in the lab. Need more integration between the various actors in the maritime world.

3. Mark Sutcliffe, MICS, Director Maritime Safety and Security Alliance CIC.
Slide 2 – shows the UK 85,000 port calls per annum, lots of ships, cargoes, people, data and money for cyber criminals to steal.
Slide 3 – globally and nationally we face the same problems. For physical crime, too many reporting channels with different forms. Poor culture of reporting which means the information flow is slow. Dialogue is very much one way and no actionable rapid information is given back. No reporting centre globally for cyber incidents.

Incident information should flow out from CSO & CISO to Captains and Crews and beyond them into their organisations, the management to the board and finally shareholders to understand the dynamic security risks and release budget.
Slide 4 – GNSS – PNT – poorly protected. 5 years ago, the IMO was requested to take action and nothing has happened.
Slide 5 – someone with a jammer can stop a ship sailing.
Slide 6 – 173 NATO warships have been spoofed. We know a collision has happened.
Slide 7 – if there is an incident then everyone needs the data. Have to develop a real-time information flow. Need to connect the world (CISOs) in real time to cyber issues and incidents.
Slide 8 – Innovate UK has given a grant for a Mental Health Awareness Alliance for seafarers.
Slide 9 – UK only circa 150 companies with around 1000 ships. The UK Government does not know who all the CSOs & CISOs are for these companies nor how well trained nor how they collect and share data. Difficult for these people to articulate the threats to crews, captains, to their management, boards and shareholders. Need to have the buy-in of the latter in particular.

Slide 10 – take briefings and produce a summary to circulate amongst CISOs
Slide 11 – CSOs like the reports and do tell the Alliance what is wanted.
Slide 12 – supply chain security is key, have a duty of care to the supply chain to do something about it.
Slide 13 – BIMCO survey – how does a company know if their supply chain is secure? Creating a standard and a dashboard for users.
Slide 14 – Alliance is working had to create the right value proposition. 60% of shipping companies have 5 ships or less so physical and cyber security officers tends to be part-time jobs as they have other tasks
Slide 15 – cannot wait for the IMO to light up the path the path. Work with partners to make sure information is verified.
Invite HMG to support all in this endeavour. With key contacts, access to resources and accelerate the development of what will be global delivery for industry

5. **Open questions and discussion –**

SF – we consider crime in a UK context. Which countries are doing this well?

AP – new legislation in different countries to contain customer information, having to look at how data can be kept in country and how to overcome different legal restrictions is a challenge.
The only country with scale and capability is the USA. 40% of global ransomware attacks are in the USA so they are easy meat. FBI were superb and helped Maersk track criminals to their base. FBI understand that they need to track the bad guys to their source.

MS – criminals share tactics, techniques etc. Partnering with AMMITEC (150 Greek CISO's) which keeps the Alliance grounded in their needs. Building cultural trust is also important as well as sharing what people want to be shared, enough but not too much. The US is the only one resourcing properly to protect their country

Prof Keith Mayes – matters seem to be much worse when compared to our first meeting. In terms of positive things that we can do, we have a skills shortage and an international problem. Chairs International Cyber Security Centre of Excellence whose rationale is to solve international problems. This is about as international as you can get! Centre has 50 experts from a number of different countries and are active in subjects that will help the maritime industry with technical issues. Wonder if we can re-run this in front of the Centre to get them thinking about the problem.

Would this be useful?

AP – we focus a lot on the vessel. Not the biggest problem as the vessel is the jumping off point for something bigger, a conduit to attacking the corporate network or the port / terminal infrastructure. Would like to take up Keith's offer.

MS – great idea, fully support it.
RH – fantastic idea, nice to work with others.

KM – How big a problem is securing legacy problems?

RH – not found solutions for this. Have managed to crack devices very easily. Big problem that needs a good response.
AP – point is that the underlying infrastructure is vulnerable. There are layers of defence that can be deployed in front of that.

Baroness Neville Jones - IMO was mentioned is it blocked by wider UN division, why is there no hope in that quarter?
Ports and terminals have a strong interest in this, what are they doing to contribute to providing safe harbour.

AP – BIMCO came up with some regulations for cyber. Part of the challenge is that everyone has to agree to a minimum standard which usually means cost. Smaller shipping companies cannot easily invest. The low bar is a struggle for many companies. Need to find a way to make it not costly esp. as we go into a Recession.

On ports and terminals, it depends on the location. We own ports and have invested but many are in the hands of smaller operators, so the cost of entry is too high. Some of the locations are geo-politically critical. May need to help specific locations to come up to standard.
MS – 120 cargo handling ports in the UK, everyone has a security officer, but everyone needs to have a cyber security officer. Code of silence that stops people sharing data etc. With a hedge fund who told the port CEO he would be sacked unless he got a grip on cyber security. It is the shareholders who lose money/value if a cyber incident is badly handled. Need incident data to be shared.

AP – cyber intelligence needs to be turned into risk data that is monetised.

Sarb Sembhi – going to Amsterdam to talk on supply chain based on an article written over a year ago. Only cyber security speaker, something is going on.

6. **Conclusions – Thanked the speakers. Will contact the Ministers responsible.**
7. **Next meeting –** December when we will be looking at the Digital Divide and cyber security