APPG ON CYBER SECURITY MEETING ON MARITIME CYBER SECURITY
MEETING MINUTES 15th October 2023 3.30 p.m.

Title: The purpose of the meeting is to explore the maritime sector and issues around cyber security.
Chairman's welcome
Present: James Morris MP, (Chair), Lord Arbuthnot, Baroness Uddin
Apologies: Lord West, Lord Mackenzie
Speakers:

1. Kevin Forshaw is Director of Industrial and Strategic Partnerships at the University of Plymouth

He has been working with shipping operators, ship builders and equipment manufacturers to build reliance against maritime cyber-attacks using world-leading thinking from the University. He is also Chair or Maritime UK South West, a clustering organisation that brings R&D active businesses together with Research base support, while working with Government to develop effective policy and support for the Region.

Previously at the UK's National Oceanography Centre and the University of Southampton, Kevin has always been at the interface between Industry and Academia, securing many millions of pounds of UK and EC R&D funding for collaborative research for the Maritime Sector in areas including maritime cyber, green shipping and marine autonomous systems. Driving innovation for new product development, Kevin set up and launched many initiatives including the UK's Marine Robotic Innovation Centre which was used as a case study by the OECD's Ocean Economy team, the outputs from which were presented at locations including the UN, and during the key note at Ocean's Week Canada 2018.

(See attached slides) Slides 1 and 2: Many ports have been hit by cyber attacks e.g. Barcelona. The US Coastguard has reported a 2021 66% increase in attacks. Most shipping operators do not understand that they have a network of technology on board ship. Massive increase in organised crime and state sponsored terrorism.

Cyber Ship lab – physical twin to a real ship's bridge. Use this to demonstrate how attacks can attack a ship.

Slide 3 – aim is raise awareness across the sector.
95% of trade is maritime based. This is why the Australian attack is critical. You could use the ship, Maersk Triple E, as an attack vector. Many ports have narrow channels of entry which state sponsored terrorists can use. Plymouth did a spear phising attack asking the captain to update the new charts from a spoof website which sits on the electronic chart display surface. In the video the crew have 2 minutes only to override the system. This is too short and the vessel runs aground.

What are the economic implications? Maritime cyber security is a real issue. Sector is not united; our ports are highly vulnerable. State sponsored attacks could find this a real weak point.

2. **Dr Konstantinos Mersinas is the Director of the Distance Learning MSc Programme in Information Security and the Academic Lead for industrial placements at the Information Security Group, Royal Holloway University of London.**

He is a Certified Information Systems Security Professional (CISSP) and a Lead Auditor in Information Security, and has worked in various information security roles before joining academia. He is a trained mathematician and has been teaching a range of academic courses, including human aspects of security, security management and cybercrime. Konstantinos is conducting interdisciplinary research in cybersecurity, behavioural economics and psychology. His behavioural experiments have been cited by the US Department of Homeland Security. He is co-founder of the Hub for Intergenerational Vulnerability to Exploitation (HIVE) at Royal Holloway. During the past years, he has served as project expert advisor for the Department for Digital, Culture, Media & Sport (DCMS) and the Department for Business, Energy & Industrial Strategy (BEIS). He is a Director at the International Cyber Security Center of Excellence (INCS-CoE.org), an initiative established between UK, US, and Japan to promote international research collaboration in cybersecurity.

See accompanying slides:
Need to look at behaviour change as much as understanding.
Lots of legacy systems, old ships and increased connectivity. Borders between IT and OT are not clear and many seafarers reporting unhappiness with their working conditions, this affects their decision-making capacity.

More complexity, highly dispersed targets combine to make it hard to secure assets and systems. The market takes time to come up to date as well. Human error is reported as the main attack vector.

We have made systems strong but not humans, so attackers aim for the weakest point. Bounded rationality theory tells us why humans are the weak point. How do we shift humans from being a vulnerability to being a defensive system? How do we utilize AI and transform people's behaviour?

Behaviour change – several models: give the individual information so that they think that they can cope with attack. Also give people a solution. The defensive stance is a bad result when people reject the message. The protection motivation is a good result.

3. Richard Preece, Chief Training Officer, OSP Cyber Academy

An experienced organisational agility and resilience 'hybrid' consultant and leader. He connects business and technical leadership of digital innovation cyber resilience and data protection. In addition to the OSP Cyber Academy, Richard is Co-Founder and Director of Toccata Data Governance Ltd and Director of DA Resilience Limited.

Key message: we are talking about trust in those who deliver services in the maritime environment. Are organisations credible, competent and authentic in their actions? Does regulation help us to trust these organisations?

Network Information Security (NIS) Regulation is a good first step. Do we trust that the Boards of companies and the regulators have the right information and understanding of the risks? Do we understand our supply chains both digitally and physically. DP World had four major ports taken offline last week by what was believed to be a ransomware attack. Attack did not have a global impact, so this points to containment. It took 3 days to get back into operation. Do we have trust in our port operators that they have anticipated this type of disruption and taken appropriate action to respond quickly and mitigate the harms? This is the acid test.

If organisations are not cyber trustworthy and our world sees more conflict, those supply chains will come under increased pressure. We have seen it in the Ukraine, we are going to have to start ensuring that we have the right levels of trust. Financial services have brought in resilience schemes. Is the NIS regulation effective for future challenges? Do we ensure that attack information is shared both nationally and internationally? How far down the supply chain should we go?

4. Major General Martin Smith CB MBE, Managing Director CyberPrism

During a 33 year military career, Martin Smith worked extensively in maritime security and maintained a strong focus on information superiority. He headed the military contribution to shipping and oil & gas security, modernised the Royal Marines' information and intelligence capability, commanded multinational counter-piracy operations and was responsible for Britain's amphibious force. He spent three periods in Afghanistan, in both command and high- level advisory roles, in addition to several other operational deployments. He commanded service personnel at every rank and left the Armed Forces in January 2018 having led the Nation's 7,000 Royal Marines as their Commandant General.

He left the Armed Forces in January 2018, becoming CyberPrism's MD in December 2019, specialising in software and client services for the protection of Operational Technology in the Energy and Government Sectors.

Operational technology in the maritime sector – this is the tech that runs industrial processes. In maritime terms we are talking about engine management, steering etc. These should be separated in a ship: crew IT, passenger IT, Bridge systems, entertainment systems with the operational technology as a separate system. We put devices between networks to protect both the perimeter and the borders between the systems. You use active measures to discover assets in IT systems normally but not OT ones. Health and safety comes into play with control of fire safety systems for instance.

In OT availability is key as the process has to continue. Confidentiality is not as important in relative terms, but integrity of systems is. We are seeing a rise in data poisoning systems. If the OT is not working properly then this has huge impacts on business, think of the Colonial Pipeline attack which compromised the visibility of data and thus raised doubts about its integrity.

Running out of people who understand OT which is leading to more automation. We need to monitor systems and

compliance constantly rather than the old-fashioned approach of clipboard management, reduce the manpower requirement and give people a 24/7 picture.

Maritime has a low threat perception and weak industry drivers. Yearns for cyber security to be a competitive advantage. In energy regulation is the biggest driver for businesses, the HSE being assigned as the auditor by BEIS has helped this. Maritime is internationalized, who therefore does the enforcement?

Open questions and discussion

Malcolm Warr – how do we join this all up? Everything is disjointed?

KF – within Fin Services they came together 15+ years ago to tackle the problem. We are not see this in maritime. Presented as a sector with wafer thin margins, very cost driven. Agree that we need to join this up to share data confidentially, share the impacts so that mitigation can be developed. IMO regulations are more guidance than law. Only the US Coastguard will ask a vessel for a cyber assessment.
Lesley Charteris – the insurance industry must be the main driver for this.

MS – Government intervention is important. Look at the Energy market, this is being driven by Govt regulation.

RP – Govt needs to start intervening as the industry is not incentivized to do the right thing. International co-operation is key. Margins are thin so companies will only take notice if they are incentivized. Needs a regulator who properly understands how to build their competence.
Baroness Uddin – this is the time to gather a number of institutions together who are concerned and inform the Prime Minister. Government to Government will be key.
Andrew Churchill – FS was exempted from NIS directives as they had strong security standards. Data Protection bill puts smart data onto Open Banking standards. Working on a system for bills of lading which will be based on the same standards. This joins up several sectors in a seamless way. It will have to include insurance. London is good at this.
Prof KM – we need the Govt to act as an umbrella. Academics have worked to bring Governments together.

Durgan Cooper – insurance has been a big driver.

RP – the insurance industry has been thinking about this for some time. The more they have thought, the higher the premiums have gone so many are self-insuring. Need to look at Cyber Re.
MS – H&S is a good example: the act works top down and has inculcated a bottom up culture.

Mark Sutcliffe – you only spend money on things that are regulated. Govt in US supports information sharing, NORMA is Norway's own information sharing system. The French Govt have created Encert. UK has 120 ports and 120 ships, we can create a fourth leg by creating a similar body in the UK.
KF – Australian Dept of Home Affairs has a robust strategy to be a cyber secure nation. Working closely with ports. Need to consider that approach in the UK. If 5 of our major ports were blocked then the UK has 3 days!
MS – confirmed 3 days. Major shipowner has 100+ incidents per week. There is a sense of urgency. Space and aviation are in the same situation.
MW – When we talk of cyber safety people listen.

RP – Availability, safety and reliability are the triad for Operational Technology and as we merge systems this will become more important. With AI these risks will increase.
Peter Thornton – send a message to the MCA so that their officers come down harder on vessels visiting the UK. Go above and beyond the EU NSI2.
Apurva Saval – is there anything that AI can help with?

Prof KM – from the perspective of how people should behave and make quick decisions, it would be a big step forward.
Rekka Babber – there is an international and a legislative piece, can this be helped by including cyber security into the leadership and training programmes?
Bill Mew – need to accept that we will not prevent everything so an emphasis needs to be put on response. We need proper training and communications around response. Developing a fully immersive game, happy to have people

look at this.
MW – just written to Lord Toby Harris on this topic. Involve NCSC in this.

RB – from a human factor very important.

RP – scenario testing is v. useful and you can anticipate the right scenarios. NCSC'S CAF is different from the US approach. Don't need a prescriptive set of compliance standards.
MS – the NCSC has embodied this in its cyber assessment framework. We just have to enforce it which is internationally very difficult.
Prof Kostas Markantonadis – what happens with the skill set gap and how do we incentivize the next generation of employees?
RP – diversity challenge, very male dominated and we need diversity of minds. We need a variety of backgrounds not just STEM.
AC – JROC (ICO, FCA, PSR) is bringing together the regulators.

KF – motivations have not changed, transcontinental ships change crews during a voyage. How do you ensure that the same training standard is maintained. The wage difference between crews is an attack vector.
AS – is there anything that is the same across countries such as CISSP?

Maxine Bulmer, CGI – as a commercial organization, need to get into schools and colleges to show youngsters what it might look like.
Meera Nayar, DfT – interested in the link between banking and insurance data. What would be the role of Lloyds registers and CARDO? What is the role of Government and how should this effect the Maritime 2050 strategy? The strategy wants to regenerate coastal communities and enables business to prosper.
KF – Lloyds Register is a classification society separate from the Lloyds insurer. Think of DNV who are pro-active in this area.
MS – Govt needs only to show interest to release enthusiasm.

PT – EU was brought in for this and want to ensure open cyber risk management. In the US you have to open up your cyber risk management process.
MS – enforcement is the answer. Does the CCT in the DfT have the teeth to bring about change?

RP – UK takes a principles-based approach. In nuclear, safety by design approach is a principles-based approach. This is a UK competitive advantage.
Prof Konstantinos Mersinas – international collaboration is key in this sector. There are many international players with an interest in raising the bar. Through international co-operation we can help to overcome some of the problems. Enforcement is also different in different places.
PT –. We could audit our ports immediately, the framework is there for cyber risk policies.

RP – if we look at counter-terrorism, they engaged in workshops to engage people and change culture. Low cost but essential component to changing behaviour. Govt can do this.
MS – we did this in many ports to rooms packed with cyber experts. Let the data do the talking and share incidents. Sharing information between ports is not allowed.
RP – challenge to Government: sectors need to be joined up. Who in the Govt ensures a co-ordination and looks at it from a national resilience viewpoint?
MN – which ports are a target in the UK?

PT – larger ones such as London Gateway and companies that can pay.

KF – ports demonstrate greater impact and all 4 of the shipping lines are being attacked but are paying up.

Conclusions

James Morris MP: some clear themes have come out of this meeting which are:

Role of Government, what might it be; regulatory alignment and consistency; workforce and skills issues; application of AI. It also needs to be joined up both nationally and internationally.

APPG ON CYBER SECURITY MEETING ON MARITIME CYBER SECURITY
MEETING MINUTES 15th October 2023 3.30 p.m.

Non-Parliamentary attendees:

Prof Kostas Markantonakis – Royal Holloway College
Dr Konstantinos Mersinas – Royal Holloway College
Maxine Bulmer, CGI
Meera Nayar, DfT
Malcolm D F Warr
Martin Smith - CyberPrism
Adrian Jolly – Institute of Corporate Resilience
Richard Preece – OSP Academy
Durgan Cooper - Juberi
Appu Saral
Bill Mew
K Campbell - SANS
Lesley Charteris
Heigor Freitas - Crest
Peter Thornton – Hill Dickinson
Simon Osborne – MSS Alliance
Andre Turville - Arxall
Simon Hughes – Cowbell Cyber.ai
Rekha Babber – Templar Execs
Chris Griffiths - Cyberprism
Mark Sutcliffe - CSO Alliance
Mike Hurst
Prof Kevin Forshaw – University of Plymouth