appg APPG ON CYBER SECURITY

Topic – Maritime Security: how are we defending our ships and ports?

5th June 2019 Room W2, Palace of Westminster

Present: James Morris MP; Chairman APPG

Lord Arbuthnot of Erdrom, Dame Pauline Neville-Jones

Andrew Henderson, Professor Keith Mayes, Secretariat, ISG, Royal Holloway

Apologies: Lord West of Spithead, Alan Whitehead MP

Speakers: Ben Ramduny (BR), Nigel Hearne (NH) and Peter Y (PY)

Speakers

Ben Ramduny, Head of Digital Security, Seadrill:

Seadrill operate ships and drilling platforms.

2014 was a game changer as Norwegians announced that 50 Norwegian oil

firms had been hacked and may have been compromised. Caused Seadrill and many in the industry to set up a cyber security function.

International Association of Drilling Contractors have set up a cyber security group. Issued practical advice and guidelines incl. risk assessment and baseline security controls. IADC also engages with Govts such as the US Coastguard. Industry wants to be responsible and welcomes co-created regulation. Need suppliers and integrators to be part of the solution and to step up and help.

BR is very focused on Operational Technology (OT) (aka. SCADA systems). These systems are designed to be isolated and this is increasingly not the case. Generally built on old OS such as Windows XP. If they are connected to the WWW insecurely, they are very vulnerable. Some of the vendors do not see security as a concern.

In the OT space, software systems, patching and security are not well understood. Concerns are:

- 2014 announcements demonstrated that nation states and criminal organisations are interested.
- Drilling in the Arctic makes the industry a target for environmental groups
- Opportunistic cyber criminals who are after financial gain.

Crews can be placed at risk and increases the change of a spillage. It is incredibly difficult to take over a ship as manual controls are in place. It is technically possible to take over a ship but very unlikely. Rigs have little data that is worth stealing.

Margins in Oil & Gas are low at the moment, not the money to spend. IT systems are well protected but OT are not.

Not all suppliers take security seriously. Historically systems were air gapped and isolated so there was no need to address vulnerabilities. OT systems contain a lot of data and the OT systems need to be connected to the IT systems to get the data out and to monetise it. Do not see OT system vendors including firewalls and other defence systems. Not enough competition to force suppliers to upgrade levels of security. Responses from vendors are poor when related to securing systems. Certain vendors have embraced security but tend to be the smaller ones. Need to remember that a piece of OT could be onboard for 20+ years and the vendors' lack of interest in addressing this is causing a problem.

Manual process can go a long way towards securing a system. Technology and automation of security can increase effectiveness. Worried about opportunistic malware taking control, not state sponsored attacks. The effect is on downtime which equates to US$3 per second in cost.

One of the challenges is how to articulate and control risk so that business leaders can understand the decisions which they need to take. Cyber people often lack the communication skills to tell colleagues what the issues are. CEO and COO level staff want to understand and BR has had to learn how to articulate risk.

Thoughts on recommendations:

1) Engage with ICS manufacturers to help them understand their responsibilities
    a. Global issue
    b. ICS manufacturers see this as a sales opportunity not a basic responsibility.
    c. Needs collaboration between vendors and customers
2) Engage with the Boards of maritime organisations to help them understand
    a. BR gets 5 minutes per month with the Main Board, too little time.
    b. Can NCSC help to educate Board members.
3) Encourage more people to go into cyber security.
    a. BR has been trying to recruit for 8 months without success.
    b. Salary inflation
    c. Tax breaks for companies who train people in cyber security
    d. Needs help to transition people from pure IT tracks to cyber security through part-time courses.
    e. Cyber security is something we all need to understand, can we add to the school curriculum?

Drilling industry wants to get involved in cyber education.

<u>Nigel Hearne, Consultant, Pen Test Partners LLP</u>

Maersk was not a hack but collateral damage.

Maritime space – lots of legislation, NIST in particular is important. DCMS' Code of Practice for IOT is a good start.

How you attack a vessel is similar to attacking any organisation. You can attack a vessel directly or via corporate HQ. NH showed SHODAN which enables you to find hardware anywhere in the world. Many Industrial Control Units are on the Internet. Many still use default user names and passwords. NR showed the position of vessels with sat comms around N Europe. The most common password is 1234.

Criminals recognise that attacks and threats are a way to make money. Many ICS can be bought online so you can take them to pieces and reverse engineer them. Found things like hard coded credentials. NH – vendors do not take IT security seriously.

U S Coastguard on the 27th May 2019 issued a note to warn about live phishing attacks. Aim is to find out the details of individual crew members so that they can be singled out, befriended and socially engineered.

Many vessels still use default credentials on legacy systems. NH demonstrated how a vessel can be "moved" by taking over the ECDIS system so it believes that it is somewhere else. If you can interfere with the messaging you could adjust the balance and the trim. Possible, yes but likely no. Ships stop slowly but turn quickly. NH demonstrated how you can change data on a ship's system and make it turn for instance in a different direction. Crews can overcome this manually but it takes time to react.

Glencore vs MSC in 2017, two shipping containers with cobalt worth £1m vanished. The agent was most likely compromised.

Vendors sell devices with the same key. NH showed a logic controller that controls steering and propulsion systems. This has no security credentials but can be used to send information back from ships to central systems and share information. This is a highly possible attack scenario.

NH no vessels visited and checked was as it was meant to be functioning. Vessels can be controlled manually but if systems are compromised and need to be fixed, it involves sending out people to the vessel.

Vendors need to be held to account. Is DCMS best practice enough, probably not?

Much better Board level awareness

Can NCSC help to share knowledge across the maritime sector?

Security should not be an option.

Peter Y, NCSC

Introduced the NCSC, not a regulator. PY has responsibility for supply chain. Maritime is part of transport which is a subset of CNI. Only has one person to look after it. No Information Exchange for Maritime. Plan to spin one up in 2019

Cyber Security Information Sharing Partnership is an online platform with 4000+ users. Have to have a UK base. 50 individuals from maritime companies are involved in CiSP. UK Network Information Systems regulations for Ports and shipping is based on NIST. Gold standard, UK focussed and can be used for US and UK firms.

PY confirmed that the views expressed about physical controls are what he sees.

Have not seen any signs that attacks are imminent. Lines are blurring between the different threat actors as they are using the same tools. Attackers use similar methods.

NCSC offers a lot of information on the main website. NCSC has created a Board toolkit. Have worked hard on this to get it right. Boards should understand enough to ask poky questions.

NCSC is trying to do something with the pipeline and are trying to intervene at the earliest opportunity such as the Girls' competition.

Engagement with manufacturers is an international problem, may need to engage via 5 eyes. Wants to pilot continuous vulnerability planning for suppliers to Government. Called Supplier Check and in pilot stage. Services, software and hardware are all international problems. How do you know that your hardware has not been tampered with?

Questions

Dan Eccles, Cyberowl – does competition get in the way of collaboration? BR – yes, involved in US ISACs and get good intelligence from there but not in the UK. Maersk's drilling platform security is market leading. Cannot talk about what they are doing! Senior management sees cyber security as something not to share.

Andy Woolhead, SANS – ex RN. 95% of imports and exports go by sea. Dangerous assumption to say is it likely, no? World is very dangerous place at the moment and things can change on the flip of a coin.

Dame Pauline Neville-Jones – does anyone know what the intentions of DCMS are regarding the Code of Conduct for IOT?

PY – still out for consultation? [Note the last day for consultation was 5th June].

SCADA systems are highly porous, SHODAN has been well known for a long time. Do the controlling minds in industry know about this? NH – not sure, vendors are there to make money. Risks are coming in as people want to extract data to understand machinery better. Fight around who owns the data: user, machine vendor, machine user. Once you take data out of a vessel you can start to plan route changes, costs of running the vessel. Vendors are not motivated.

Colin Gillingham NCC, Industry should be telling the vendors what it wants.

BR – customers all want to do this in the drilling sector. No leverage on suppliers. Cannot go to them and force them to do it.

Prof Keith Mayes, RHUL. Need to shoot down the reliance on the airgap, just takes one rogue crew member. Vendors need to show how they deal with the threat

Anu Kharmi Templar Executives – set up Int Maritime Security sector group as they see a lot of tech start-ups working in this sector. Singapore Govt recognised the importance of this. Are seeing different things happening in maritime, concerns over the introduction of technology vs long established practices. The leadership agenda and training is key. How often are people trained in cyber security?

NH – seeing more awareness posters on vessels.

BR – two levels of training at Seadrill. One for all staff and one for hands-on management staff for the IC systems.

Rory Hopcraft RHUL – is there merit to what the IMO has done to put the cyber risk assessment into the standard vessel certification? Could the IMO push back if these are generic problems.

NH – people go deaf at the mention of cyber security but not cyber safety.

AK – kitemark for cyber security?

Dame Pauline Neville-Jones – More mandation is needed.

IOT is global.

NH – you can buy a child's watch to track your children. Watches are generic and vulnerable to attack.

Dan Eccles – sounds as if the issues that maritime are facing are not being dealt with across the sector. Are you interested in engaging with other sectors?

BR – No. Hard to put your own solutions onto systems.

Dame Pauline Neville-Jones – have Lloyds been active?

John Head, Paragon Insurance – UK is playing catch up with the US. US insurance industry has evolved much more than ours.

PN-J – good relationship between insurance company and client.

NH – Lloyds bought Nettitude to make money from this.

AK – Govt document Maritime 2050 is a good document which covers the ground. Insurers often do not cover cyber security.

Conclusion Meeting closed at 19.00. James Morris thanked the speakers and participants. The APPG will draw up a list of issues and review these further.