IALA WORKSHOP ON CYBER SECURITY

WORKSHOP REPORT

12, 15 to 19 November 2021

Virtual workshop

Jaime Alvarez
2021
Workshop Secretary

19 November

10, rue des Gaudines – 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01 – Fax +33 (0)1 34 51 82 05 – contact@iala-aism.org
www.iala-aism.org
International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

This page intentionally blank

Report of the workshop on Cyber security

Executive Summary

The workshop on Cyber security was held on 12 November 2021 and from 15 to 19 November 2021 as a virtual IALA workshop. The workshop was attended by 64 participants plus three members of the IALA secretariat. The list of participants is attached as **Erreur ! Source du renvoi introuvable.**. The Chair of the workshop was Phil Day and the hosting country was Canada.

The working group 1 considered the human factors in cyber security for AtoN and VTS.

The group identified organisational gaps and cyber security threats and proposed high-level mitigations.

It was recommended that cyber security should become an integral part of the day-to-day business.

The Working Group recommended the following key items of further work for IALA:

- Identify appropriate cyber security guiding principles and apply these in IALA guidance documents and courses
- Review IALA toolbox of risk assessment to include cyber security risk

Working Group 2 considered the platforms and subsystems within the scope of IALA and identified areas where IALA could have a key role to play in implementing protection and mitigation measures.

Key vulnerabilities were identified as positioning, navigation and timing (PNT) systems and the automatic identification system (AIS).

The Working Group recommended the following key items of further work for IALA:

- A Recommendation for IALA members on how to apply the concepts of security by design to both radio and electronic AtoNs and all platforms that include telemetry, remote administration, edge devices or Supervisory control and data acquisition (SCADA) systems, and
- To consider how authentication, authorization & encryption can be applied to the systems within the scope of IALA and what the priorities are for these.

The working group 2 proposed mitigations and protective measures and proposed further work for IALA to address these and other cyber security issues within its scope of work.

The working group 3 discussed post-operational cyber incident response and business continuity. Most important conclusions regarding business continuity are that cyber security risks should be incorporated in existing business continuity plans.

With regards to planning for cyber incident response the working group determined that scenarios for cyber incidents should be developed, in particular for AtoN and OT systems. Furthermore, a clear policy and incident response plan should be established.

In handling cyber incidents, first response is the organisation's own responsibility, for further analysis, forensics and assistance in recovery, a specialised 3rd party is recommended. For information sharing, the working group suggested that IALA may be facilitator for an ISAC (Information Sharing and Analysis Centre).

Contents

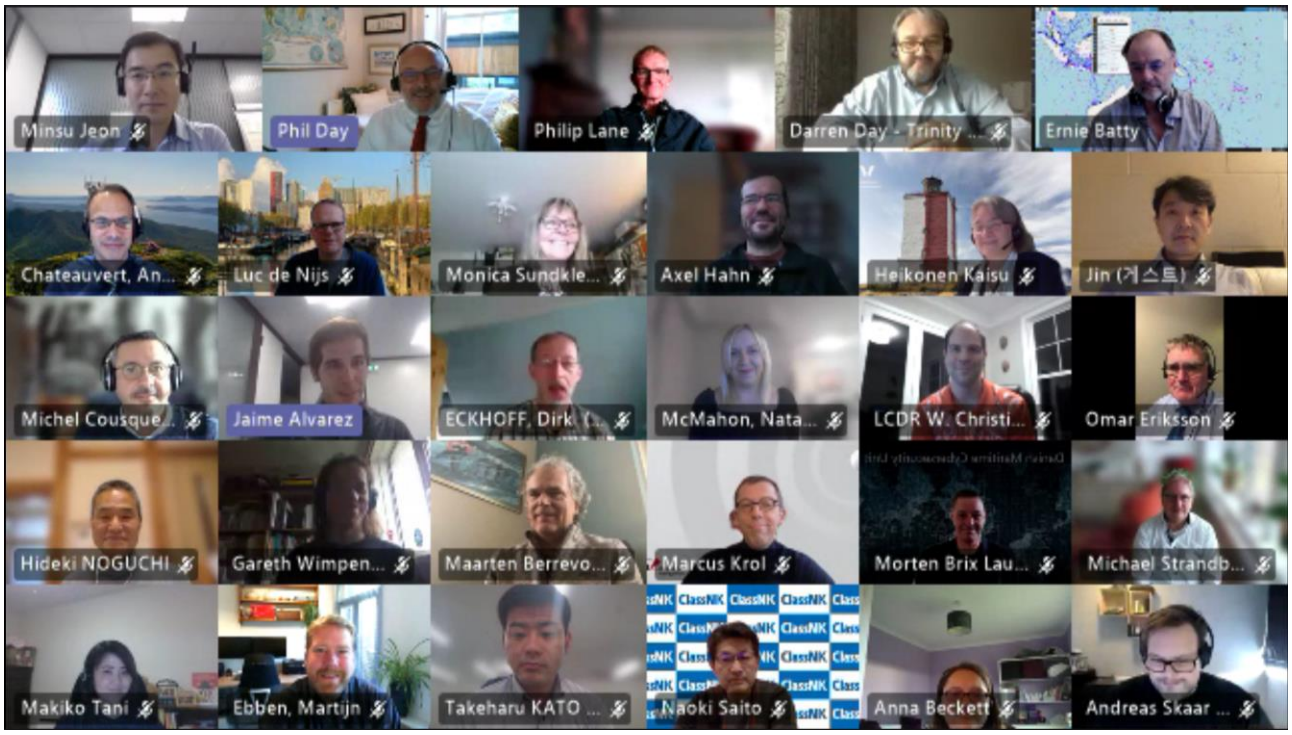
List of Figures

List of Tables

Report of the workshop on Cyber security

1. INTRODUCTION

The workshop on Cyber security was held on 12 November 2021 and from 15 to 19 November 2021 as a virtual IALA workshop. The workshop was attended by 64 participants plus three members of the IALA secretariat. The list of participants is attached as **Erreur ! Source du renvoi introuvable.**. The Chair of the workshop was Phil Day and the hosting country was Canada.



Workshop participants were provided with the working arrangements and tools available for the exchange of documents, communications between participants, conduction of presentations and discussions.

The dedicated website for the workshop is https://events.iala-aism.org/iala-events/workshop-cybersecurity/

1.1 Working program of the week and expectations

The Chair introduced the programme for the week (ANNEX B) which also can be found on the workshop website. The workshop was divided into three main blocks:

- the kick-off session informed all participants about the aims and goals of the event and how the workshop was structured. The kick-off session provided guidance information for participants on the tools which would be used during the workshop.
- presentations and discussions from a range of expert speakers covering topics related to cyber security, including terminology, technologies and status in other organisations and the general sharing of views and opinions; and
- the working group sessions where the participants were split into three working groups:
    - WG1 chaired by Rene Hogendoorn, Stefaan Priem and Jillian Carson-Jackson and instructed to consider that cyberattacks against critical infrastructure are very often mediated through human behaviours or deficiencies in operational or security processes; current level of maturity of cyber security processes and user education in AtoN and VTS operators; Identify important industry-wide gaps in organisational security policies and cyber security awareness and priorities for addressing these gaps; among others

- the WG2 chaired by Philip Lane and Jin Hyoung Park are instructed to consider relevant technologies in operating Marine AtoN, including VTS; Identify the most vulnerable systems whose security should be addressed in priority; cyberattack scenarios against AtoN, VTS or related systems that would adversely impact maritime operations; Identify priority corrective measures on known vulnerable technologies based on risk; Identify "security by design" approaches that could be adopted in the context of Marine AtoN provision; among others
- the WG3 chaired by Martijn Ebben and Hideki Noguchi is instructed to consider the response and guidance during and after a cyberattack event for the different operations and systems impacted; Identify business continuity approach and scenarios during and recovering from a cyberattack; Identify existing business continuity best practices to be considered within the marine AtoN and VTS operation;

Further information is detailed in the terms of reference (ToR) document available in the programme section of the website.

1.2 Presentation of input papers

Under this agenda item, the documents were presented which were proposed to be read by the participants to start the discussions with the latest updates, and useful information produced by the IMO, BIMCO, other organisations and IALA Committees. Other useful links to guidance documents on cyber security were published in the pre-reading section of the website.

2. SESSION 1 - OPENING OF THE WORKSHOP

Phil Day, Chair of the ARM Committee and chairing the workshop, opened the first session introducing briefly the programme, logistics and the number of experts that will be setting the scene for the upcoming working sessions.

2.1 Welcome from IALA, Francis Zachariae - IALA Secretary-General

Francis Zachariae welcomed participants to the workshop on cyber security highlighting that even if the virtual event is not the preferred option, the cyber security matters needed to be covered before the end of the work plan. Secretary General and the Secretariat really hope that the events planned for next year can be in person in Saint-Germain-en-Laye or elsewhere in the world as the members are used to. It is really needed.

First, Francis Zachariae thanked the Canadian Coast Guard for hosting the workshop which was supposed to take in place in Quebec. Also, a big thanks to all the people involved in this workshop. The Chair Phil Day and all the working group chairs, speakers, and participants. An amazing group of specialists and experts contributed to the work during the week.

IALA and its members have always tried to identify threats impacting the maritime services. This is not new. It could be weather, climate, visibility etc, but in an increasingly connected and technologically dependent world, new areas of vulnerability are emerging. Cyber security is a difficult subject and very difficult to understand and more importantly to do something efficient about. A bit like global warming. Lots concern and many words, but unfortunately fewer concrete actions. Francis Zachariae looked forward to being a bit more specific when it comes to the cyber threat related specifically to IALA business – AtoN – after this workshop, so that all members can benefit from future guidance and best practice. IALA members have the great advantage that in IALA is not political and is focused on technology and solutions in the best interest of safety. A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. So, a very serious threat specially when the trend is to become more digitalized in VTS, MASS, e-Navigation, virtual AtoNs etc. The matter should be considered very seriously, but also listen to all the guidance from other sectors who are much more targeted than IALA. The financial sector, aviation, the military, and the public sector. After all, the threat to AtoN is probably not as high, but the members need to understand how high and what to do.

Francis Zachariae looks forward to the outcome of the workshop. Specially to understanding the threats and the level of threats better and how the committees can better take this into account in the future work. Francis Zachariae thanked again for the continued dedication of those who host, have planned, and attend this coming week for the time you give to ensure that the committees can work more efficiently with cyber security.

Looking ahead, the Workshop on Enhanced Radar Positioning System (ERPS) will start at the end of November 2021. A subject that could also be of interest for this group.

2.2 Welcome from Canadian Coast Guard, André Chateauvert – Canadian Coast Guard (CCG)

André Chateauvert welcomed all participants to the virtual meeting. He raised the point to develop process and procedures to report, face and recover from cyber incidents inside the maritime organisations and administrations. A lesson learnt process should also be implemented in order to hardening organisations again future attacks. CCG considers cyber security as a key element due to the increase of infrastructure and system supporting marine navigation through a digital perspective within the AtoN programme, marine traffic and communications system providing VTS and eNavigation services. André finally recalled the importance of the workshop outcomes, not only for the participants and IALA members but also for the mariners.

2.3 Cyber Security in the maritime domain, Jose Fernandez - Bastionnage

Jose provided insights on the various cyber threats that could affect the maritime domain, actors and vulnerabilities as well as scenarios and finally inherent challenges for the maritime user. José started the presentation defining some terms need to know before starting the discussions: qualitative and quantitative risk, targets of attacks being the information assets and other terms related with undesired outcomes. It was identified the scope of cyber security in organisations: external actor and internal threats. The scenario of an outside threat follows typically the procedure of identification of the server (application, server among others) → penetration → exploitation of such lack of knowledge from the user and other take advantage of the different vulnerabilities. Cyber security also defines the threats into these technological domains including hardware (laptops, servers, net equipment, and cloud) and software (Windows/Linux). Mass market cybercrime remains a challenge for the individuals' users. The computer operator/owner feels the consequences, the incentive to mitigate the ransomware is higher than other modes of cybercrime. Cyber sabotage made by subversive groups and targets organisations. Finally, the third kind of cyber threat to traditional IT includes the cyber supply chain since the hardware is asymmetry manufactured over the world but also software threats in supply chain also occurred. The question raised on the supply chain risk in the maritime domain. José also spoke about the physical cyber domain or CPS (Cyber Physical System) and its different elements. It was highlighted that there is a limited number of companies manufacturing both hardware and software of generic ICS / OT. The supply chain for those systems is therefore easier to define and secure than generic IT. IoT and IIoT (Industrial IoT) is a current trend and subject to cyber threat to generic CPS. Looking specifically to the IT and OT applying to the maritime domain, the following table was presented:

Table 1 - IT & OT in the maritime domain

	Shipping	Ports	Aids to navigation	Ships
Traditional IT	- Computer networks (IP, wired/Wifi) - E-mail - Document management & DB - Web applications - Electronic payments			

Domain-specific IT	- Ship tracking
	- Shipment tracking
	  - Manifests
	  - RFID
	  - *Blockchain*
		- Scheduling
		- Truck control
			- Vessel Traffic Services (VTS)	- Chart updates
				- Pax/Crew Internet

CPS	- RFID - AIS	- RFID - Physical access control - Surveillance	- Marks & lights - Buoys - Radar beacon - AIS AtoN - Surveillance Radar - …	- IPMS - ECDIS - AIS - Radar - Sonar - …

A view of the potential actors in maritime was also proposed:

Table 2 - Potential actors in maritime cybersecurity

Potential impact	*Cui bono*
• Disruption of maritime shipping (long term) w/ severe economical impact	• State-level actors • Subversive groups
• Catastrophic destruction (shipping incidents)	• Terrorist groups • State-level actors
• Disruption of maritime surveillance operations (short term)	Organized crime • Smuggling/drug trafficking • Illegal migration • Cybercriminals (extortion)

Some vulnerabilities are recognised in the AtoN including VTS management and operations: AIS, Racons among others could be spoofed (signal and information). Therefore, this is a possible scenario of cyberattack. The hacking of AtoN equipment is also considered a plausible scenario. Jose identified the challenges of maritime cybersecurity based on the lack of common language and understanding of the work and priorities across these three groups: IT/Cyber security personnel – AtoN / VTS operators or experts – Maritime operators. Another challenge is that the solutions have permitted to avoid or mitigate attacks in the past and the methodology to recover is well know as well as the risk. Thus, the cyber security professional is placed in a comfort zone. However, the countermeasures do not cover targeted domain specific attacks, more sophisticated, non-money motivated etc. Also, a challenged to Jose, is the fact that AtoN / VTS have no suffered major attacks, the possible implication when attacking these assets are unknown etc.

Finally, Jose concluded that most important cyber risks are placed on Ransomware (targeting critical infrastructure IT (non-maritime-specific)); AIS/Radar spoofing (on a State-level or subversive actors causing short to mid-term disruption to shipping); Hacking of AtoN systems. He also provided a prioritisation:

1. Rapid adoption and introduction of secure technologies (→AIS)
2. Cybersecurity standards for AtoN and VTS products
3. Human factors (vector for ransomware; how to handle events and recover)
4. Achieve generic IT cybersecurity maturity in the organization
5. Domain specific cybersecurity solutions

2.4 Cyber Security in other bodies, Jakob P. Larsen – BIMCO

Jakob provided a presentation on Maritime Cyber Risk Management and the recent publication from BIMCO *et al* on such matter. It is important to highlight that according to IMO resolution MSC.428(98) *Maritime cyber risk management in safety management systems,* shipping companies should include cyber risk management in the safety management system and not in the ship security plan. By the time of the DOC audit in 2021, all companies / administrations should have put in place the procedures to ensure that cyber risks are appropriately addressed in safety management systems. The risk assessment procedures were stressed, and the principles are described in the ISM Code 1.2.2. Jakob presented an example of an approach from a shipping company addressing the managing of cyber risk with all the specific procedures, forms and list to complete.

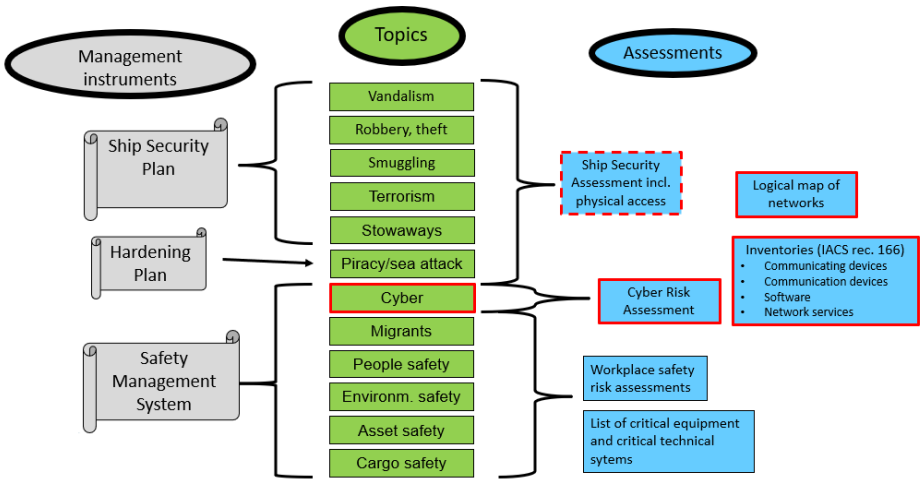


Figure 1 - Structure of the approach from a shipping company on cyber risk managing

As part of BIMCO recommendations included in their guideline, the development of a logical map of networks on board and inventories of all different types of IT and OT equipment (permitting controlling operational systems) should be considered. Based on these two inputs, a risk assessment is established. Jakob put the heads on the necessity to investigate the concept of risk to develop the risk assessment. The breakdown of the different elements of risk are presented in the formulae below:

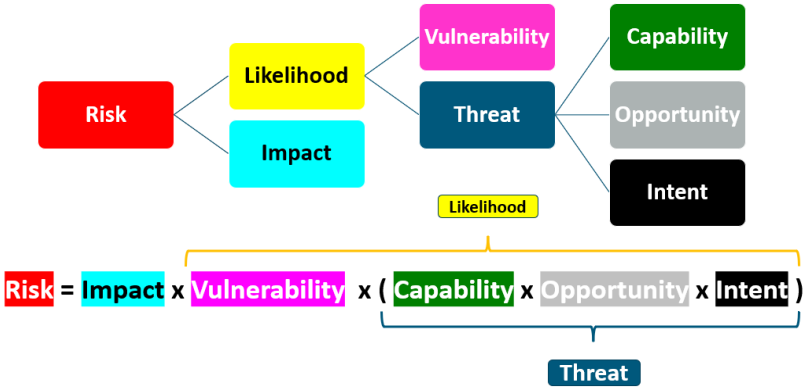


Figure 2 - Risk calculation and breakdown of elements of risks (BIMCO)

Some examples were provided on capability, opportunity, and intent. In this specific maritime case: ships could take advantage in the intent because of the more limited access of a hacker to the ship. A risk matrix was also presented as an example in conjunction with the use of bridge equipment as ECDIS. The following recommendations on immediate steps were addressed:

- Map remote accesses and data flows
- Segregate networks: critical systems, admin, crew, passenger
- Protect access to shipboard computers and systems (firewall, password management, removable media ports, physical access control)
- Protect email and other internet facing systems and software (antivirus)
- Initiate awareness training of all staff

Jakob finally provided the status of cyber risk management: No major ship cyber-related incidents with severe impact to humans, ships, or environment, a rapidly changing situation and the consequent need for continual improvement.

2.5 Cyber Security in other bodies, Jonathan Pritchard – IHO

Jonathan Pritchard provided a presentation covering the matter of standard evolution for data protection and data integrity and how they are recast into the IHO S-100 framework as well as how cybersecurity is impacting on that implementation. It was recalled that the history of IHO Standards has considered the data protection and authentication in the ECDIS (IHO S-63) as part of the data protection scheme permitting to be authenticated and even encrypted by an accredited data server (ECDIS digital chart provider). Using digital signatures and 40bit blowfish encryption among other capabilities aims at avoiding data corruption and reflects the cyber security matters when implementing digital data on ECDIS and such data in transit. Jonathan also referred to the latest updates on S-100 IHO's Universal Hydrographic Data Model which is being implemented as part of the new generation of electronic charts (more products, enhanced interoperability…). S-100 Part 15 is included specifically for data protection of S-100 (data encryption and digital signatures for authenticax²tion). S-100 will also be interoperable with various technical standards for data security / integrity used in mainstream internet technologies (X509). A revised type-approved S-100 ECDIS will be available for such purpose.

A diagram presented in slide 6 showed how IMO and IEC standards fit together and are inputs to the S-100 with the goal that all data imported into the ECDIS will digitalised signed (the origin for it can be checked on the ECDIS) and optionally some of them could be encrypted for copy protection. For instance, related to the data coming from the AtoN network, the AtoN service provider would be authenticated by IALA who is internally authenticated by IHO. Thus, the IHO data protection scheme will provide the identity certification to the data available in the bridge. In consultation with different maritime stakeholders setting the different use cases for S-100, interoperability of data is also sought with a view on future uses as well. The latest revision of S-100 Ed.5 will come out in 2022 and will be the basis for the revision of IMO performance standards for ECDIS to include S-100. An overview and roadmap of IHO standards and its implementation on the ECDIS was provided:

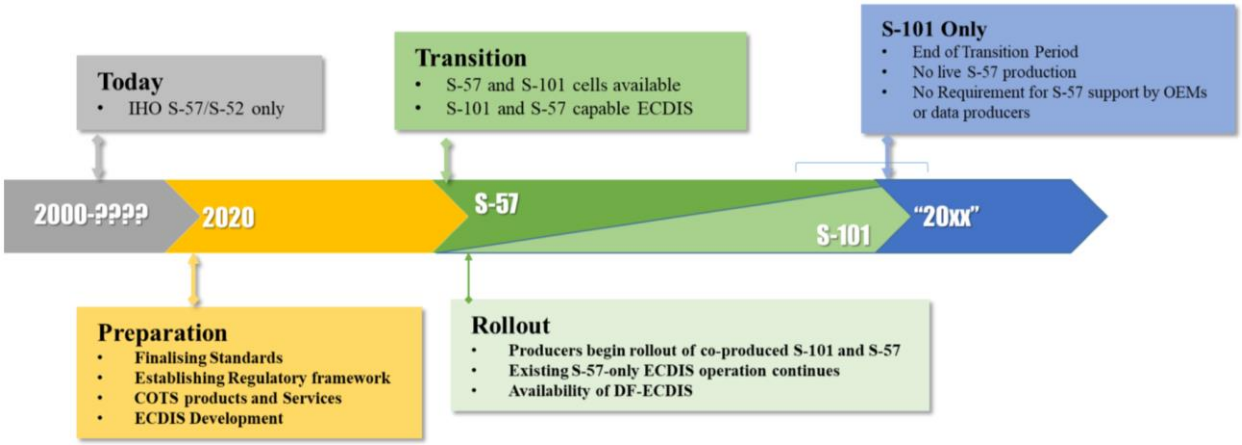


Figure 3 - Roadmap of IHO standards and its implementation on the ECDIS

3. SESSION 2 - PRESENTATIONS AND DISCUSSION WITH EXPERT SPEAKERS

Session two was chaired by Dirk Eckhoff, VTS Committee vice Chair.

3.1 Cyber security for e-Navigation platforms, Axel Hahn – OFFIS/DLR

Axel presented the role of e-Navigation platforms on cyber security. He also highlighted the fact that technologies used for AtoN including VTS are not secured against cyber threats (AIS, GNSS and ENC, GMDSS, VTS and logistics). It was highlighted the threats of eavesdropping and data manipulation (including data manipulation on physical channel and impersonation). It was presented a spoofing scenario over AIS data. Axel stressed the different objectives and are of improvements in terms of confidentiality, integrity, availability, authentication, and authorisation. Public key encryption is seen as a technology very needed providing encryption from a key of a transmitter to a user who also have the same key. FAL application is also suitable for encryption mechanism. The authenticity of navigational warnings remains the key to data. Digital signatures (public and private keys) by the authorities will be required and get storage and made available on a very secure place/way. Here is where e-Navigation platforms play a major role; As recalled, the maritime

services are typically provided by an e-Navigation Platform being a system that facilitates secure and reliable exchange of information and services (as defined in IALA G1161). The requirements for such platforms required to have a way to detect services and secure identity management. The criteria for e-Navigation platforms are based on efficiency, robustness, and resilience. IALA G1157 and IEC 63173-2 are also reference documents. Axel finalised his presentations stating that Internet technologies are part of the solution of cyber security and digital e-Nav Platforms make a secure information exchange possible – for the first time.

3.2 Cyber security for AtoN, Jens Ohle – Sealite

Jens started the lecture informing about the historical development of AtoN monitoring based on human observation at first then to a connected solution but remaining closed systems (PSTN → RF → GSM). Currently, a convergence on IT and OT technology and based on IT methods network design in line with the following trends: proliferation of IoT using IT networks, Traditional OT / SCADA networks have now merged with IT networks and with the characteristic of making possible the accessibility to these networks anywhere. RF Networks substitute the public switched telephone network (PSTN) allowing area of services not covered, last mile solution, for ISM band no regulatory approval but got congested. GSM services provided reliable service and became the industry standard for many applications; however, the coverage is still poor. The proliferation of IoT increased the need of low power RF devices and Bluetooth and Zigbee became popular for communications but with a limited coverage. Satellites were little by little used in line with the decrease of their cost of operation. The global coverage and type of constellation (LEO / MEO /GEO) directly impacting on the latency of the data are important factors to have in mind when considering the user requirement. These developments on technologies have impacted on the applications permitting automatization, remote and reliable monitoring, reduce maintenance and reach availability targets. For an AtoN operator or manager, the number of monitoring assets have increase largely which imply deliberate cyberattacks on business and infrastructure: petrol stations, pipelines and power stations are targets of these cyberattacks. Energy, transportation, mining, and construction are top targeted domains / activities suffering cyberattacks. The technology used for data transfer is subject to such threat: GSM, Bluetooth, PSTN, Wi-Fi, TCP, RF on different ways of data corruption. The need for encryption is therefore needed to keep the risk of AtoN operations as low as possible. Another risk to AtoNs' is accidental due to the human factor, data corruption and connectivity risk (interference). The reason for hacking were stressed being ransomware the most observed. Jens presented Iridium as the preferred technology for last mile communication and the data management platform to mitigate the risk permitting different capabilities and methodologies as part of the design considerations (encryption levels, segregation of Personally Identifiable Information (PII), authentication among others). Jens advised that good procedures could be to conduct penetration testing not only for system validation, but continuously, maintain backup and restore management and finally to start by forming a written IT cybersecurity policy for risk mitigation.

3.3 Cyber security for VTS, Ernest Batty - IMIS Global Limited

Ernest provided the history and overview of past and current cyber security threats as depicted in the picture below (2020):

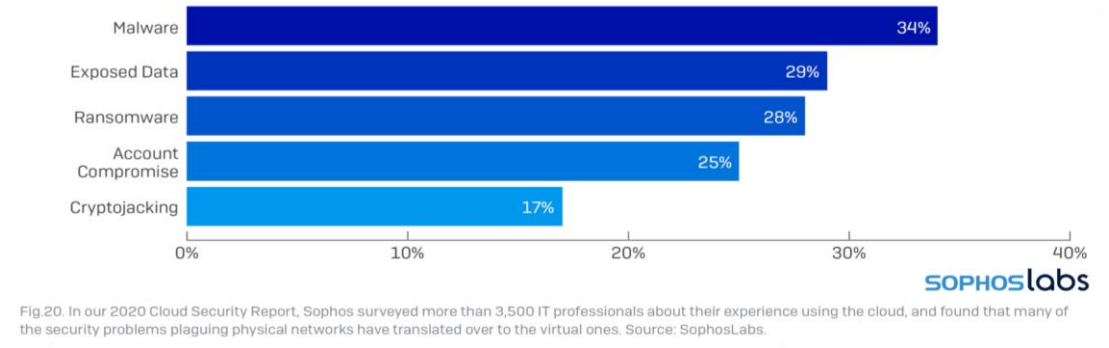


Figure 4 - Organisations suffering security incidents in the last year

Then, he exposed the statistic that AtoN including VTS operators and designers should consider in terms of average time to identify and contain a breach, data breach lifecycle, parameters and conditions involved in

the attack. A calculation of the economic impact also showed the high impact in the industry of such events. Threat and vulnerability are key terminology to be understood and differentiated in the AtoN / VTS cyber environment. The level of knowledge of vulnerabilities from others and the VTS is key to determine the threat:

Figure 5 - Threats and vulnerabilities

The Zero Day threat of vulnerability is a software vulnerability discovered before the VTS vendor has become aware about it. Hackers explore these vulnerabilities which causes high impact. Ernest informed about the external and internal character of vulnerabilities (split again on non-human and human and again in intentional / accidental). Other terminology was also defined as attack surface and attack vectors. A system the more connected is, the more attack vectors have. The increase of complexity of VTS systems with the system integration leads to an increase on connectivity that also imply a distributed environment where the equipment or subsystems are no longer in the same room. Therefore, a relation between the increase of the complexity and the attack surface is created:

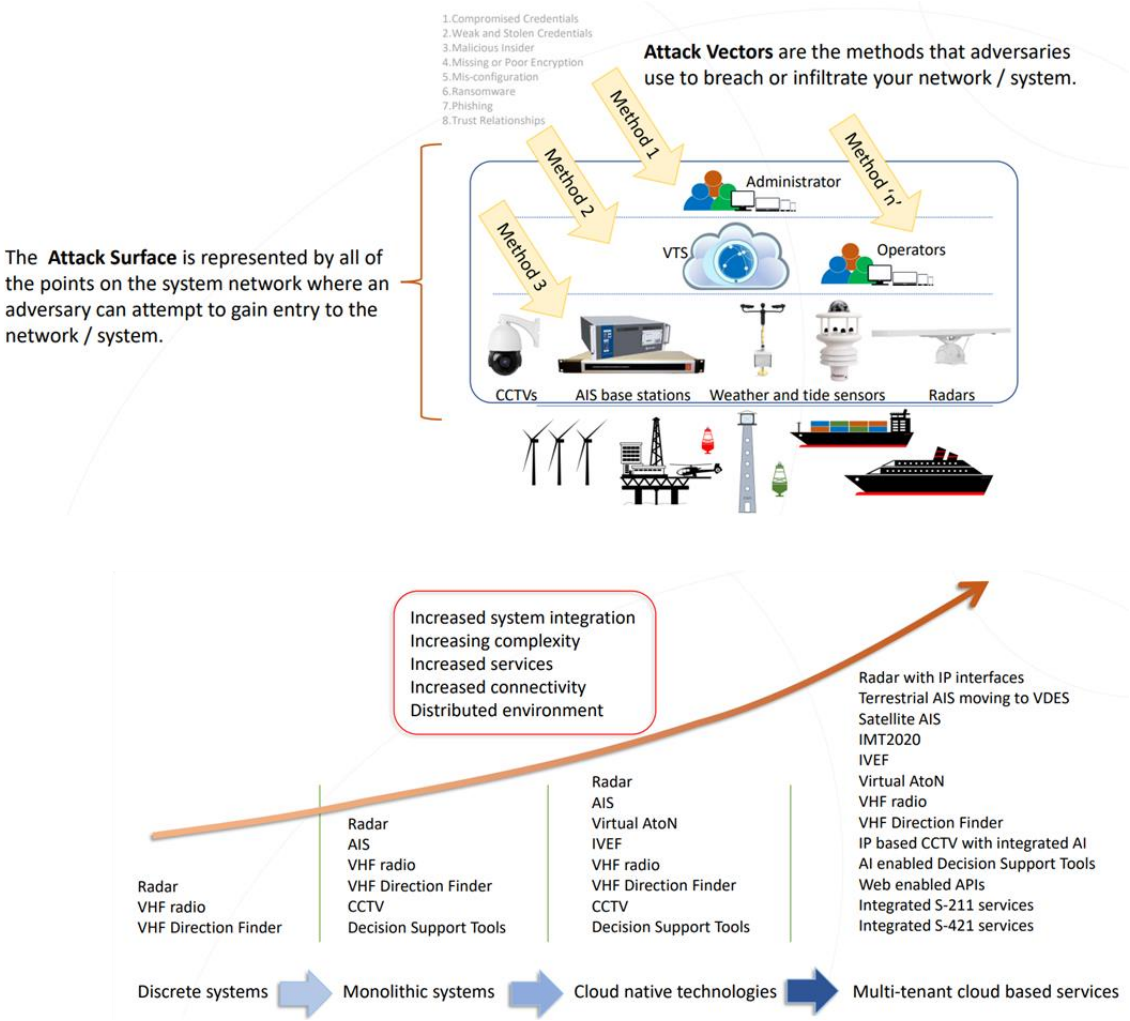


Figure 6 - Relation between VTS complexity and attack surface/vector

Future VTS systems could include an increase of services using AI, a connection with external services, sharing of data with larger port community (using Application Programming Interfaces – API), the use of high bandwidth, mobile phone and even the inclusion of MASS. IoT is also expected to grow support on VTS services which imply attack options to hackers. AI has also a role to play on Decision Support Tools which will include external data from a wider data source → increasing of data surface / data vectors. Ernest pointed out the availability of cyber security guidelines (BIMCO, NIST, IAPH, EU Agency for Cybersecurity). The scheme defined in NIST guideline is the preferred one for the speaker and could be implemented in the cyber security framework for VTS. Ernest finally raised the question on what could be done in the short term in the VTS to stress the cyber security matter:

1. Assume Zero Trust.
2. Create strong VTS user access protocols
3. Use strong authentication policies
4. Protect the VTS backups
5. Segment the VTS network
6. Monitor the VTS network / system

3.4 Question and answer session

- A question related to Jakob's presentation – about the number of cyber incidents on ships that have not been reported or published. *As per BIMCO view there are not many attacks with serious implications that have not been reported. The importance should be given to the capacity to recover from them instead. Seafarers do not often experience such events neither.*

- Could we add GNSS vulnerability too as a cyber threat? *Definitively, GNSS signals can be fake and spoof. Aviation is very concerned on this, and criticality could be less in maritime. It is observed a motivation from operators to fake GNSS signals.*
- Are insurances considering cyber risk disclaimer on discussion in the maritime domain? *Distribution of risk is considered – increasingly used and BIMCO has developed a cyber risk clause distributing the risk between the ship owner and the charter putting responsibilities between them.*
- A question on saying S-100 supports 'full strength' 128-bit crypto algorithms, rather than 40-bit? If so, has this caused difficulties with US 'ITAR' restrictions on the international stage? *Correct, 128-bit AES is used. The expert believes ITAR certification isn't an issue for it (no states or OEMs have raised an issue). Specific exclusions for AES-128 or better. Old S-63 was 40 bits to get over the US export restrictions. Interested to know if this is an issue - none of IHO US/CA members have raised it yet.*
- It was mentioned API like tidal heights being interfaced through S100. Does IHO see a range of equipment e.g., anemometers or say RACons being interfaced to the ECDIS or would IHO expect this to be related to chart related features? *These are certainly possible as S-100 enables both API based interfaces to be made to the ECDIS, and multiple datasets to be specified for import. It would require a specification to be made for data to be interfaced under the framework. There are no barriers to doing this - if there is a use case then it should be possible for the relevant domain body to specify how it is done. There's obviously a risk of clutter and "too much" data on the ECDIS though which needs to be borne in mind. The features can be linked to the chart features as well....*
- What is the view regarding having multiple last mile systems being enabled on AtoN e.g., IR, Bluetooth should those not being used be switched off? *Any active connection can be prone to attacks, so if the technology is not part the monitored solution / or control solution, then it should be switched off to minimize any attempt of attack. Malcolm added There is also sequencing. i.e., You need to enter a code or PIN to access or read data.*
- Is the process described by NIST on cyber security protection already been established in any VTS over the world? *Cyber security policies have implemented these metrics at design level and during the training of the VTS Operators.*
- Are research and innovation projects on networks considering from the beginning the cyber security threats? *Identity is key on the developments of new technologies. Also, a good selection of technologies available for the maritime domain and a correct use of them remain extremely important to cope with cyber security matters.*

4. SESSION 3 - PRESENTATIONS AND DISCUSSION WITH EXPERT SPEAKERS

Monica Sundklev Chair of the VTS Committee, moderated session three of the workshop.

4.1 Preventive measures to ensure Cyber Resilience, Alan Jacobsen - German Waterways and Shipping Agency

Alan provided guidance on preventive measures to ensure cyber resilience inside the German WSV but with a view on being used by other organisations anywhere. He first informed about the security organisation, roles, and responsibilities, therefore, how the staff is structured and what their tasks are in relation to security. The process approach was then addressed focusing not only on IT security but also on a holistic approach (from business processes and including IT, assets, organisation, and staff). It is required to define the protection levels of applications and the implication on business processes. The implication of the Information Security Management (ISM) is also needed and addresses again some roles and responsibilities to the staff organisation when dealing with a new application. In parallel, different operational procedures should be followed to prove the adequate implementation of such new application and keeping in mind the security requirements. Alan also informed about the role of the ISM on already in use applications and systems. In both cases (new and in use app/syst.), a catalogue of security requirements for buildings, servers, clients, change management should be produced and maintained. At this point, two types of requirements are set up: main requirements (compulsory to be implemented) and other requirements (risk is acceptable – not compulsory to implement). Addressing the human element, a few points were suggested to raise the

employee awareness on the cyber security topic. Finally, the question on handling security incidents was stressed considering procedures, security staff availability, reporting channels, action timing and final responsibilities and decision-making within an organisation. The first response to an incident will then conduct to: crisis management / business continuity / recovery.

4.2 Incident Response and Recovery, Martijn Ebben - Port of Rotterdam

Martijn provided insights on cyber incident response and stressing the fact that the probability for an organisation of being impacted by a cyber incident is very likely as ransomware. The correct human behaviour could help to avoid these incidents but zero risk would never happens. A good preparation would then been needed to effectively recover from a cyber incident. Martijn presented a methodology to face a cyberattack with different steps that should be well known by the staff and prepared to be applied immediately. Noting and reporting the actions conducted to mitigate the risk is also important, the number of people involved in this event response should then be enough to act and take notes to later investigate. Some preferred actions were exposed as well, and the crisis management team should be also established on beforehand. A good business continuity plan is required since part of the business network will be switched off or no longer useful. The incident recovery which will provide the ability to get back to the business requires several technical solutions and checking to make sure that the incident is still not located in the system. Most organisations choose to hire this as a service. The reporting at this stage is vital to avoid coming across the same mistakes in the future. Then, Martijn tailored this general view on cyber incident response and recovery to the AtoN, including VTS, and maritime services in the context of eNavigation. A few questions were raised looking at the impact of cyberattacks to the AtoN and maritime services operations. An example of AIS spoofing o Gulf of Corsica confirming the high vulnerability of AtoN and maritime services. Alternatives to normal technologies used could be put in place as for AIS → Radar and CCTV ; VHF → Telephone and audio visuals signs ; GNSS → bearing and distance positioning and time synchronisation via LTE

4.3 Cyber Security Risk Management in the maritime domain including the human element, Jose Fernandez – Bastionnage

Jose started the lecture briefing about risk management, strategies to address risk and risk managementwhat the countermeasures or controls should be deployed. High level approach.

As part of the managing of risk, the analyse of risk before considering any countermeasures should be put in place for each potential threat. Thus, dealing with the determination of the scenario and actors but also calculating quantitatively the risk. Risk reduction can be due to the reduction of probability (i.e., protection or detection countermeasures) or the reduction of impact (i.e., backups). Another parameter to ponder when choosing and introducing countermeasures is the cost of ownership (acquisition and operation) and to calculate the return of investment (ROI). Part of the risk management activities is to apply the management principles, that is, to prioritise countermeasures either risk-based (those with highest risk reduction) or protection-based (those with best/shortest ROI). Selection between these two options are very much related to company policy. Jose introduced the standards or frameworks on cyber security applying to risk management:

- ISO/IEC 27001 with the oldest and most common IT security management standard. Describes “process” to become more mature in terms of cyber risk management. However, does not describe what the countermeasures or controls should be deployed. High level approach.
- NIST Cybersecurity Framework, which has become very popular, is aimed at critical infrastructure providers (more detailed descriptions and activities / comprehensive language for non-cyber experts) and identifies five main security functions:
    - Identify
    - Protect
    - Detect
    - Respond

- Recover

Considering specific maritime domain standards, the following ones could be consulted:

- Generic: IMO – Guidelines on Maritime Cyber Risk Management (April 2017)
- Ports: IAPH - Cybersecurity Guidelines for Ports and Port Facilities (Version 1.0) – July 2021
- Ships:
  - Various org. (BIMCO, ICS, WCS, etc.) – The Guidelines on Cyber Security Onboard Ships - 2021
  - ABS – Cybersecurity Implementation for the Marine and Offshore Industries (Feb 2021)
  - ABS – Cybersafety and Cybersecurity certifications

On the AtoN/VTS side, no guidance has been produced yet.

Jose recalled the structure within an organisation in the scope of cyber security which will be in coordination or even merge to security on a whole (personal + physical + cyber).

4.4 Question and answer session

- It was recalled during the discussions that the CIA requirements also apply to non-IT components, including AtoN. Integrity and Availability of AtoN are key elements to ensure navigation safety.
- A concern related to the issue of merging of business system with operating system was raised. The trend is to combine both and converge in the same network as this is cheapest and could be beneficiary for cyber security to trace the operator/user who has access to the operating area physically and by the computer.
- Comments were made on the document from ISO/IEC 27001 which helps with establishment of an ISMS (Information Security Management System) and ISO/IEC 27005 which specifies the standard for Security techniques and for Information security risk management.
- A question was asked to Martijn's presentation regarding why procedures should be printed in paper although most quality systems today are being only kept in electronic format (online). *Documents such as emergency procedures for cyber security should be on paper as well as something that is very sensitive for the organisation as the procedures may not be accessible in case of a cyberattack.*

5. WORKING GROUP SESSIONS - IALA GUIDANCE AND ROADMAP

5.1 Working group 1 - Preventative procedural measures and behaviours

5.1.1 Executive summary

In considering preventative procedural measures and behaviour for cyber security, Working Group 1 (WG1) considered the human factors in cybersecurity for AtoN and VTS.

WG1 identified gaps in current procedures and training, proposed mitigations for those gaps, identified threats and measures to prevent operational disruptions. Finally, WG1 considered how to create and foster a cyber-security culture, where cyber security is acknowledged and integrated into the day-to-day business.

The group recommended the following

- **Recommendation 1**: It is essential to raise awareness, implement procedures related to cyber security, encourage good cyber-security behaviour and provide regular training;
- **Recommendation 2**: Cyber security roles/profiles and associated responsibilities should be assigned throughout the organization;
- **Recommendation 3:** Cyber security should be part of the management culture throughout the whole organisation, and become a standing agenda item as an element of maintaining a safe and healthy work environment;

- **Recommendation 4**: Cyber security must be embedded into the life cycle management of systems.

5.1.2 Introduction

Working group 1 on Human Factors and Cyber Security met on 16, 17 and 18 November 2021. The Group was chaired by René Hogendoorn and vice-chairs were Jillian Carson-Jackson (Nov 16) and Stefaan Priem (Nov 17 and 18).

Based on the presentations, comments and questions made at the plenary, WG1 was instructed to:

- Consider the current level of maturity of cyber security processes and user education in AtoN and VTS operators;
- Identify important industry-wide gaps in organisational security policies and cyber security awareness and priorities for addressing these gaps;
- Identify cyber security management standards that could be adapted and adopted to ensure proper cyber security governance in AtoN and VTS operations;
- Identify which preventive and detection measures should be prioritised;
- Identify desired behaviours, including safety and security culture;
- If possible, propose topics that may be considered in future IALA work programme for IALA Committees regarding the preventive technical measures; and
- Submit a report to plenary by 18 of November 2021.

5.1.3 Discussions

5.1.3.1 Current level of maturity of cyber security system processes

After reviewing the topic, the group concluded that there was too little common ground among the diverse systems to be able to establish a "current situation". For that reason, the group did not pursue this topic any further.

5.1.3.2 Industry-wide gaps in organizational security policies and awareness

The group identified the gaps. These are provided in Table 3. The gaps are identified based on the priority assigned to the gap during the discussion of WG1.

The table identifies

- The gap;
- The (high-level) options to mitigate the gap;
- The dependencies that need to be addressed before the mitigation option can be exercised; and
- The perceived priority of addressing the gap (high – medium – low).

5.1.3.3 Cyber security management standards

Based on the opening presentations it was noted that there are many different cyber security management standards. To assist with the focus of the discussion, WG1 invited Jose Fernandez to provide additional information on this matter.

Following discussion, it was noted that cyber security is an organisation-wide concern and applies to people of different domains (both OT and IT). All people within an organisation need to understand and use a common cyber security language. The cyber security terminology and processes must be accessible to all people, regardless of their background.

The NIST framework provides a reasonable approach to providing this commonality of terminology and is an existing standard. This standard appears to be a suitable starting point for further IALA work. In this context, the work of ENISA may also be relevant.

5.1.3.4 Preventative and detection measures

WG1 considered cyber security threads related to malware, ransom ware, unauthorised access to data, unauthorised access to physical locations, phishing, failure to keep systems up to data, unintended

consequences form system updates, incorrect configurations, conversion processes to new platforms, receiving unreliable data from external systems, system vulnerabilities and system overload.

The results of the review are provided in Table 4. The table includes:

- The identified threat;
- The possible impact if the thread results in a breach;
- Measures that can be taken to counter the threat or identify a breach, resulting from the threat;
- The domain of the measures in NIST terminology.

Note that the identified measures relate to the human factor. No technical measures were considered as they are in the domain of WG2.

5.1.3.5 Fostering a cyber security culture

For the human factor in Cyber Security, WG1 noted that the most important issues are

- Raising awareness, encouraging good cyber-security behavior and (regular) training;
- Assign cyber security roles/profiles and associated responsibilities throughout the organization;
- Cyber security should be part of any meeting agenda and part of maintaining a safe and healthy work environment;
- Consider what's in it for the individual and how to make this part of the daily routine/contribution (initial training to bring everyone at the same level followed by moving to business as usual);
- Cyber security must be embedded into the life cycle management of systems.

Table 3 – Gap Analysis, priority, and options to address

Gap	Explanation of Gap	Options to address	Priority	Dependency
Insufficient awareness	• operational persons not aware of how cybersecurity affects 'me' (for others, not me) • understanding / realization of the consequences • Difference between home systems / work systems	Training Develop procedures	High	• Management engagement • Policy • Inventory and risk assessment
How we think of data	• Think of data differently / understand more about how data can be used effectively (protection of data) • change mindset to support data, benefit for all - so no single point of knowledge / single point of failure. • Awareness of individual roles with engaging with cybersecurity aspects		High	• Management engagement • Policy • Inventory and risk assessment
Procedural	• requirements for physical access to the system (user controls, common access card, …) • desired behaviors to physically protect the system and related infrastructure • prevention of unauthorized remote access to the system and related infrastructure • procedures during and post incident (e.g. system shut down) • distinction between home systems and work systems (mixture of both) • work from home, access to the systems	Develop relevant procedures Create/promote a cyber security culture Training Engineering controls (design of systems to minimize human error) Built-in processes Implement a system for quality assurance	High	• Management commitment • Cross-organizational and seamless collaboration • Clear distinction of roles

Gap	Explanation of Gap	Options to address	Priority	Dependency
Different age of systems	Older systems (existing systems without cyber security) and newer systems • i.e. S-100 Part 15 will have security included • retrofitting existing technologies for cybersecurity / working with new systems that have security built in • dealing with legacy systems and newer systems.	Identify previously unknown risks that were not addressed earlier in the systems (risk assessment) Implement controls for systems that were not designed with cyber security in mind	High	
Knowledge Transfer	• When people leave the organization, how to address the access? • The concept of 'corporate knowledge' when people leave / the cybersecurity knowledge • physically removing access to the system, but how to address the 'knowledge' that someone takes with them.	Awareness Training on procedures Ensuring critical information is maintained within the organization on how to update/maintain the systems Identify undocumented workarounds that should be documented as procedures	Medium	
Financing data to protect database	How to ensuring funding / financial support for cybersecurity? • need to evaluate the data you have / look at how to highlight the value of addressing cybersecurity • value of the information / value of protecting the information • separating the database from the infrastructure that houses the database	Monetize data value and identify and inform on the cost of the consequences (data loss/theft, disruption of services) Include data value in the risk assessment IALA toolbox for risk assessment	Medium	• Awareness • Management commitment
Language related to cybersecurity	• providing cybersecurity in a common language, removing the 'jargon' and making the language more accessible (regardless of the background) • NIST terminology, BIMCO, etc. (Rene put a document on the file share - members to look to	Raise awareness Training	Medium	

Gap	Explanation of Gap	Options to address	Priority	Dependency
	this). (note - general thought - why develop anything new when there are other standards that exist - i.e. NIST which appears to be complete). • Conclusion (17/11): use the common language of NIST as a starting point/outline which may lead to an IALA guideline			
Generational Differences	• Comfort level with technology, awareness of cyber security aspects (different risk thresholds), different levels of trust in the tools	Address training for different generations • methods to use • level to 'pitch' this • provide a spectrum of approaches	Low	Part of training
Transferring data from legacy to new platforms	In the transfer to S-100 / vulnerabilities • moving from what we know to what is coming • need to address these vulnerabilities / developing the transition. • humans looking at how the work with the data base • transferring existing data to a new standard • procedures, training, attitude on attention to detail	Awareness Establish realistic time-frames for transition	Low	
Different guidelines	looking at different guidelines, IAPH, BIMCO, IALA • Helping the human navigate the landscape of existing and developing guidelines with regards to cybersecurity, training, cyber hygiene, etc. • Which guideline for a base (discussion on NIST / ISO / etc) and importance of the selection of the framework (NIST or ISO or other) and promote training of this framework to create a common language.	Harmonization through development of IALA guidelines for ATON and VTS	Low	

Table 4 – Preventative / detection measures and procedures

Threat (malicious or unintentional)	Impact	Preventive/detection measures	Purpose (NIST framework)
Malware	Virus, unauthorized access, system lockdown, data theft, loss of confidential information	Create awareness through (regular) training, virus protection, procedures (limit to software that can be installed and by whom)	Identify Detection Protection (through software)
Ransom ware	System lockdown (no access for the organization unless ransom is paid) and financial damage	Create awareness through (regular) training on organizational level, procedures for recovery,	Protection Recovery
Unauthorized access to (confidential, sensitive or protected) data	Data theft, corrupt/amended or loss of data	Define access profiles, define the ownership of the information	Protection
Unauthorized physical access by employees or visitors (server rooms, equipment rooms, standalone network devices, operational rooms, remote locations)	(Un)intentional system disruption, data theft, unauthorized remote access,	Procedures for access, access restrictions, locked and monitored rooms and locations, procedures for visitors	Identify Detection Protection
Phishing (more focused on the human element, targeting individuals (one or in mass))	Virus, unauthorized access, system lockdown, data theft. (on both the individual level and the organizational level)	Awareness and training (test emails) on what it is and its possible impact, procedure for follow-up	Detection Protection
Failure to keep systems up to date (not installing patches/updates)	Virus, unauthorized access, system lockdown, data theft, system disruption	Procedures to keep the systems up-to-date and a policy/culture on that (e.g. inventory)	Detection Protection
Unintended consequences from system updates (patch that may hinder/break down the system)	Workarounds, system break-down, system disruption	Procedures (testing patches in a separate system), policy of risk matrix	Identification Detection Protection

Threat (malicious or unintentional)	Impact	Preventive/detection measures	Purpose (NIST framework)
Incorrect configuration	Virus, unauthorized access, system lockdown, data theft, system disruption	Training, regular tests, procedures for development and deployment process	Detection Protection
Conversion process to new technology/software/platforms/…	System not accessible, unintentional access, system failure	Training, regular tests, procedures for development and deployment process	Detection Protection
Receiving unreliable data from external systems (e.g. AIS, Bluetooth)	Integrity of the system	Awareness, procedures and training how to deal with the data and to correlate data, procedures to detect incorrect data, identify authorized sources	Identification Detection Protection
System vulnerabilities through design and standard that are easy to spoof or jam (e.g. AIS)	Integrity of the system, system disruption	Awareness and understanding of the full-spectrum of the implications, training, procedures to adapt to the situation, back-up of the system	Identification Detection Protection
System overload (e.g. botnet attack)	System disruption (affecting the system in a negative way)	Awareness and understanding of the full-spectrum of the implications, awareness of the roles, training, procedures to adapt to the situation, back-up of the system	Identification Detection Protection

5.1.3.6 Topics for future IALA Guidance

WG1 recognised the work already underway with regards to cyber security, human factors and ergonomics. The group proposed the following topics for future development within IALA:

- Review IALA toolbox of risk assessment to include cyber security issues;
- Consider the human factor aspects of cyber security in the development of the draft IALA Guideline on Human Factors and Ergonomics in VTS;
- Include cyber security in IALA documents such as training model courses for AtoN and VTS and operational and technical guidelines;
- Identify appropriate cyber security guiding principles, measures and behaviours for AtoN and VTS.

5.2 Working group 2 – Preventative technical measures

5.2.1 Executive summary

In considering preventative technical measures for cyber security, Working Group 2 (WG2) identified vulnerable systems, proposed mitigations and protective measures, and proposed further work to address cyber security within IALA's scope of work.

While platforms and equipment within the scope of IALA are subject to the same threats and vulnerabilities as systems in the wider world, WG2 identified positioning, navigation and timing (PNT) systems and the automatic identification system (AIS) as particular systems where IALA could have a key role to play in implementing protection and mitigation measures.

A major vulnerability identified by the Group was the lack of authentication, authorization and encryption in many of the systems within the scope of IALA. While the Group noted that it might not be appropriate to apply all three of these measures to all systems within the scope of IALA, the Group took the view that there is a pressing need to ensure that authentication is built in to new systems and products.

The Group recommended the following corrective technical measures:

- **Recommendation 1:** Regarding GNSS reliability, continue to support the work of ENG WG3 and ENAV WG2, while informing their work in the context of the wider cyberattack threat.
- **Recommendation 2:** That IALA underlines (e.g. through a cyber security guideline document) the importance of securing IT against traditional threats as a priority goal (organisational goal), ahead of finding and deploying solutions for AIS security (which needs an industry-wide effort).
- **Recommendation 3:** That IALA underlines and recommends to its members that they make themselves aware of existing AIS and GNSS spoofing and jamming detection and mitigation capabilities in COTS VTS, employ them in the most efficacious manner in their operations and provide a guideline on how to protect against other similar threats, e.g. camera signal spoofing, etc.
- **Recommendation 4:** That the need for an industry-wide effort, possibly initiated by IALA, be discussed at the highest decisional level of the IALA organization.
- **Recommendation 5:** That IALA set up a task force to define a path towards finding, adopting and deploying a long-term robust solution to AIS message authentication.
- **Recommendation 6:** Inform and adjust objectives of ENAV WG 1 (Digital Information Systems) to include the exploration of cryptographic solutions that would support the use of PKI in low bandwidth applications.
- **Recommendation 6.1:** Suggest to ENAV WG1 that it should look at IEC to update IEC 63173-2 SECOM (S-100) (supporting IP-based communication) to support other non-IP data exchange technology, e.g. AIS, VDES, etc., by liaising with the IEC Work Group working on this (IEC TC80 WG17).

5.2.2 Introduction

Working group 2 on Preventative Technical Measures met on 16, 17 and 18 November 2021. The Group was Chaired by Philip Lane and the Vice-Chair was Jin Hyoung Park. A Subgroup on Priorities for Corrective Technical Measures was Chaired by Jose Fernandes.

Based on the presentations, comments and questions made at the plenary, WG2 was instructed to;

- Consider technologies in operating Marine AtoN, including VTS;
- Identify the most vulnerable systems whose security should be addressed in priority;
- Identify cyberattack scenarios against AtoN, VTS or related systems that would adversely impact maritime operations;
- Identify priority corrective measures on known vulnerable technologies based on risk;
- Identify "security by design" approaches that could be adopted in the context of Marine AtoN provision;
- Identify detection technologies and procedures;
- identify organisations that are dealing with cyber security in the critical infrastructure and/or maritime context; existing standards covering cybersecurity and carry out a gap analysis in the scope of IALA;
- if possible, propose topics that may be considered in future IALA work programme for IALA Committees regarding the preventive technical measures; and
- submit a report to plenary by 18 of November 2021.

To help guide their work, the Group received presentations on paper ENAV28-5.1.1.4 (*The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards*) and the key points from the plenary presentations on technical countermeasures and cyber security frameworks such as that set out by the United States National Institute of Standards and Technology (NIST). During their work, the Group also considered the Guidelines on Cyber Security Onboard Ships, Version 4 (BIMCO et. al.), the USCG Cyber Strategic Outlook and IAPH Cybersecurity Guidelines for Ports and Port Facilities.

5.2.3 Discussions

5.2.3.1 Relevant Platforms and Related Technologies

The group identified the following marine AtoN platforms and related sub-systems and technologies as within the scope of IALA's work on this topic:

- **Physical AtoN** (buoys, beacons, lighthouses)
    - Hardware – signaling equipment; specifically light & sound.
    - Physical access
    - Monitoring, control & telemetry (including communications protocols, networks and channels)
    - Telematics and remote administration (including software updates and device configuration)
    - AIS & GNSS
- **VTS**: The Group noted that VTS consists of a wide range of technologies to deliver its tactical and strategic functions. The following list was derived from IALA Guideline G.1111 (*Preparation of Operational and Technical Performance Requirements for VTS Systems*):
    - Radar
        - Radar with IP interfaces

- AIS-networks
  - Terrestrial AIS moving to VDES
  - Virtual AtoN ?
- Environmental monitoring
  - hydro-meteo sensors
- Electro-optical systems
  - IP-based CCTV with integrated AI
- Radio Direction Finders (RDF)
  - VHF Direction Finder
- Long range sensors
  - Satellite AIS
- Radio Communications
  - VHF radio
  - IMT2020
- Data processing
- VTS Human / Machine Interface
- Decision Support
  - AI enabled Decision Support Tools
- External Information Exchange
  - Inter VTS Exchange Format (IVEF) => S-210
  - Web enabled APIs
  - Integrated S-211 services
  - Integrated S-421 services

- **Electronic AtoN:**
  - AIS
  - GNSS and augmentation systems

5.2.3.2 Priority/vulnerable systems

In considering which were the most vulnerable systems whose security should be addressed as a priority, the group identified the following:

- **Radio AtoN:** there is no authentication for AIS message 21 (Aids-to-navigation report),
- **Electronic AtoNs:** public GNSS and GNSS augmentation systems have no authentication; e.g. AIS message 17 (DGNSS correction data),
- For all platforms that include **telemetry, remote administration, edge devices or Supervisory control and data acquisition (SCADA) systems** which include interfaces to other networks, particularly public networks present an attack surface; for the platforms identified in section 5.2.3.1, they are often unprotected and have no authentication.

The Group noted that **E-Racons** are currently under development; this presents opportunity to apply security measures into the design of the system.

5.2.3.3 Cyberattack scenarios

The group identified the following cyberattack scenarios against AtoN, VTS and related systems that could adversely impact maritime operations:

- The Group recalled spoofing and jamming incidents that have already happened throughout the world, which point to the potential for attacks to positioning, navigation and timing (PNT) systems. Such actions can lead to piracy, theft, fraud, collisions, accidents, loss of property and life. PNT vulnerabilities would have an impact on all of the identified priority systems.
- A physical or virtual AtoN could be used for spoofing or DoS attacks against both physical and electronic AtoNs; causing disruption to safe navigation or VTS operations
- Interfaces to external systems for telemetry, remote administration, SCADA and data processing of VTS systems via edge devices or VTS backbone, makes them vulnerable to untargeted cyberattacks. Note: compliance with S-100 provides some mitigation for this.
- AIS used for ground surveillance could be attacked (e.g. by generating a large volume of false data representing spoofed ships). The Group noted that although radar is still a key approach for vessel detection, AIS is required for vessel identification. Also, AIS plays a different role depending on the location for example, in areas where there is no radar available it is the only option.

5.2.3.4 Priorities for Corrective Measures

A subgroup of WG2 was formed to discuss priorities for corrective measures. The following is a report from that group.

Participants: Jose M. Fernandez (Bastionnage), Jean-François Coutu (Canadian Coast Guard), Ernie Batty (IMIS Global) and Jin Hyoung PARK (KRISO).

The subgroup agreed three most important corrective measures, in order of priority due to the associated risk are:

1. Countermeasures to address GNSS signal spoofing and jamming
2. AIS message authentication
3. Deployment of Public Key Infrastructure (PKI) -

For each of these the discussion and recommendations were as follows:

1. GNSS reliability

The ongoing work of ENG Working Group 3 (PNT Resilience) and ENAV Working Group 2 (New Technologies) are already addressing this issue.

Recommendation 1: Continue to support the work of ENG WG3 and ENAV WG2, while informing their work in the context of the wider cyberattack threat.

2. AIS security

- The deployment of new standards in the VHF Data Exchange System (VDES) will not address message authentication and will not solve the AIS spoofing problem.
- There already exist several proposals by national authorities and academia to implement authentication in AIS that should be considered. This includes similar proposal to secure the "cousin" protocol in aviation ADS-B.
- It is recognized that there exist capabilities at the software level in existing COTS VTS that can detect several types of AIS spoofing. However, such methods cannot prevent AIS channels, receiving hardware or data streams being flooded with spoofed messages.

- There seems to be a gap in efficient and commercially available spoofing detection and prevention capabilities at the hardware level and in AIS data integration platforms (e.g. signal processing level, multilateration).
- It is recognized that while AIS spoofing is a serious and hard to solve problem, there are other cyber threats to VTS that are equally important in terms of risks and that more easily addressable, in particular traditional cyberattack by hacking IT components of VTS.
- Finding a solution to implement message authentication in AIS requires an industry-wide effort that will take time, but that is nonetheless crucial, and that IALA has a key role to play in "getting the ball rolling".

Recommendation 2: That IALA underlines (e.g. through a cyber security guidelines document) the importance of securing IT against traditional threats as a priority goal (organisational goal), even ahead of finding and deploying solutions for AIS security (which needs an industry-wide effort).

Recommendation 3: That IALA underlines and recommends to its members that they make themselves aware of existing AIS and GNSS spoofing and jamming detection and mitigation capabilities in COTS VTS, employ them in the most efficacious manner in their operations and provide a guideline on how to protect against other similar threats, e.g. camera signal spoofing, etc.

Recommendation 4: That the need for an industry-wide effort, possibly initiated by IALA, be discussed at the highest decisional level of the IALA organization.

Recommendation 5: That IALA set up a task force to define a path towards finding, adopting and deploying a long-term robust solution to AIS message authentication.

3. PKI

- ENAV Working Group 1 on Digital Information Systems is already working on the establishment of PKI to support exchange of information through Web applications.
- There is a technical difficulty in using such a PKI for message authentication in low bandwidth applications such as AIS or VDES, for which several solutions have been proposed in other domains (e.g. aviation) and that should be considered.

Recommendation 6: Inform and adjust objectives of ENAV WG 1 to include the exploration of cryptographic solutions that would support the use of PKI in low bandwidth applications.

Recommendation 6.1: Suggest to ENAV WG1 that it should look at IEC to update 63173-2 SECOM (S-100) (supporting IP-based communication) to support other non-IP data exchange technology, e.g. AIS, VDES, etc., by liaising with the IEC Work Group working on this (IEC TC80 WG17).

5.2.3.5 Security by Design

The Group suggested that the following “security by design” approaches could be adopted in the context of marine AtoN provision:

- **AtoN and VTS operators** should implement security by design concepts such as defence in depth.
- **Vendors of AtoN and VTS products** should:
    - implement concepts such as a secure development lifecycle (IEC 62443-4-1), secure hardware architecture during the design, development and manufacture of products,
    - consider the security of their supply chain, e.g. requiring proof of origin of components, and
    - use the principles of vendor risk management (VRM), as well as industry and national guidelines to identify high risk vendors which represent a high risk of information loss.

Supplier-specific vulnerabilities
The group noted the following regarding supplier-specific vulnerabilities:

- The increased role of software and services provided by third party suppliers to a greater exposure to a number of vulnerabilities that may derive from the risk profile of individual suppliers.

- The risk profiles of individual suppliers can be assessed on the basis of several factors, notably:

    - The likelihood of the supplier being subject to interference from a country. This is one of the key aspects in the assessment of non-technical vulnerabilities. Such interference may be facilitated by, but not limited to, the presence of the following factors:

        - a strong link between the supplier and a government of a given third country;
        - the third country's legislation, especially where there are no legislative or checks and balances in place, or in the absence of security or data protection agreements;
        - the characteristics of the supplier's corporate ownership;
        - the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.

    - The supplier's ability to assure supply.
    - The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

- The assessment of a supplier's risk profile may also take into account notices issued by national authorities.

5.2.3.6 Detection technologies and procedures

The Group noted that a new task proposed to the ENAV committee at ENAV27 to develop a Guideline for AIS/VDES VDL integrity monitoring (ENAV28-12.3.1 WG3 New work items proposal 20211015) would be a valuable contribution to address a key vulnerability of the AIS/VDES VDL.

The Group recalled the presentation at ENAV 28 by Mr. John Fischer of Orolia on Maritime Interference Detection and Mitigation (IDM) for GNSS. Mr. Fischer introduced multiple measure that could be used to detect and mitigate jamming and spoofing GNSS signals:

- Using passive upward facing GNSS antennas to mitigate against spoofing and jamming signal from low angle (from the horizon) and below the GNSS antenna (i.e. vehicles on ferries),

- Using active GNSS antennas to reject interfering GNSS signals,

- Using processing techniques to detect that a GNSS spoofing and / or jamming signal is present and warn the users of this status,

- Use of alternative PNT sources, and

- Use of multiple GNSS sources.

In summary, using suitable passive and active GNSS antennas along with PNT data processing or other intelligent means may be used to monitor sensors and data sources to provide a consistent and resilient data set. This supports measures against jamming and spoofing of data.

5.2.3.7 Related standards and organisations

The group identified the following organisations that are dealing with cyber security in the critical infrastructure and/or maritime context:

- **IMO:** In June 2017, at its 98th session the Maritime Safety Committee (MSC) of the International Maritime Organization (IMO) completed the approval of **MSC-FAL.1/Circ.3** (*Guidelines on Maritime Cyber Risk Management*). At the same session, MSC also adopted **Resolution MSC.428(98)** (*Maritime*

Cyber Risk Management in Safety Management Systems), in June 2017. This resolution required cyber risks to be addressed in safety management systems by 1 January 2021.

An update to MSC-FAL.1/Circ.3, (Revision 1) was approved in 2021. The IMO Guidelines on Maritime Cyber Risk Management are set out in the annex of **MSC-FAL.1/Circ.3/Rev.1**. The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities.

- **IEC:** The International Electrotechnical Commission (IEC) prepares and publishes international standards for all electrical, electronic and related technologies.

  The international industrial security standard **IEC 62443** covers both organizational and technical aspects of security. The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS (industrial automation and control systems) and to apply necessary mitigations in a systematic, defensible manner. The IEC 62443-4 series specifies the process requirements for the secure development of products used in industrial automation and control systems. Within this series, **IEC 62443-4-1** sets out secure product development lifecycle requirements and IEC **62443-4-2** specifies technical security requirements for IACS components.

  Work is in progress at IEC on a new standard for secure communication between ship and shore (SECOM). Publication of **IEC 63173-2** (*Maritime Navigation and Radiocommunication Equipment and Systems-Data Interface – Part 2: Secure communication between ship and shore (SECOM)*) is expected to be in June 2022. IEC 63173-2 will specify service interfaces (APIs) for data exchange and data protection measures to enable secure communication; it will be applicable to products that use the IHO (International Hydrographic Organization) S-100 Universal Hydrographic Data Model; other data formats will also be supported.

- **ISO:** The International Organization for Standardization (ISO) is developing a new Maritime Cyber safety standard (**ISO 23806**) which will provide requirements for designing, implementing, maintaining and ensuring the safety of ships operations by managing the cyber risk of operational technical systems. ISO 23806 is intended to help shipowners to update their ship safety management systems (SMS) to meet the ISM-code as instructed by the IMO resolution MSC.428(98).

- **NIST:** The United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the **NIST Cybersecurity Framework**) can be used to help identify and prioritise actions for reducing cyber security risks. It is intended as a tool for aligning policy, business and technological approaches to managing cyber risks.

  In February 2021, NIST released **NISTIR 8323**: *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*. More information here: https://www.nist.gov/pnt.

- **Shipowners and Operators Associations: The Guidelines on Cyber Security Onboard Ships** (BIMCO et al.) provide guidance on cyber security and compliance with IMO MSC.428(98). Version 4 of the Guidelines was published in December 2020, and endorsed by the IMO's Maritime Safety Committee at MSC 103 in May 2021 by means of MSC.1/Circ.1639.

- **IALA**: Recommendation **R1017** (Resilient Position, Navigation And Timing (PNT) sets out recommendations on PNT resilience for IALA members and other authorities providing marine aids to navigation services.

5.2.3.8 Gap analysis

Noting the findings of their discussion, the group carried out a gap analysis within the scope of IALA, with the following findings:

Gap	Current situation	Options to address

AIS false reporting detection	Some detection systems are available, but they are proprietary, protected or commercially sensitive.	IALA has a role to play in shaping policy on the recording of vulnerabilities and their detection.
Authentication, authorization and encryption	Authentication, authorization and encryption are lacking in many of the systems within the scope of IALA	Analyse how authentication, authorization & encryption can applied to the systems within the scope of IALA and what are the priorities.

The Group recalled that there was a patent related issue related to IALA's work on AIS base station detection this could be a useful reference for IALA's work on AIS false reporting detection.

5.2.3.9 Suggested topics for the IALA work programme

The Group propose the following topics that may be considered in the future IALA work programme for IALA Committees regarding the preventive technical measures:

- a Recommendation for IALA members on how to apply the concepts of security by design, considering the following:
    - **For AtoN and VTS operators** this should include security by design concepts such as defence in depth.
    - **For AtoN and VTS product vendors** this should include concepts such as secure development lifecycle (IEC 62443-4-1), secure hardware architecture during the design, development, and manufacture of products. Noting the supplier-specific vulnerabilities set out in section 5.3.2.5.
- how can the Confidentiality, Integrity and Availability (CIA) triad be integrated into the systems within the scope of IALA?
- how can authentication, authorization & encryption can applied to the systems within the scope of IALA and what are the priorities for these? (e.g. for GNSS, authentication may be a priority as these are free and open services, which could make the implementation of authorization & encryption impractical),
- how can new resources such as the Maritime Connectivity Platform (MCP) and the VHF data exchange system (VDES) be used in IALA's work on this issue? e.g:
    - the use of the MCP for authentication in general, and
    - the use of VDES for authentication of AIS.
- a wider gap analysis between the existing IALA instruments and standard requirements, considering the vulnerabilities, detection methods and mitigations identified in this report.

The WG noted the ongoing work at IALA on the integrity of the VDL, and considered this an essential element of IALA's work on this subject.

5.3 Working group 3 – Incident response and recovery (post operational)

5.3.1 Executive summary

The workshop was held from 15 to 19 November 2021 with the working group session conducted 16 – 18 November, chaired by Martijn Ebben and vice chaired by Hideki Noguchi.

The focus of working group 3 was a post-incident response and recovery. The issues in accordance with the Terms of Reference (see ANNEX C) were also considered by the working group.

The group identified the following key points:

1. **Business continuity approach and scenarios**
    - Cyber security risks should be incorporated in existing business continuity plans
    - Scenarios for cyber incidents should be developed, in particular for AtoN and OT systems
    - Legacy systems, especially in AtoN operations, should be considered, both as a risk and as fall-back for automated (computer) systems
2. **Existing business continuity best practices**
    - Business continuity should be organised organisation-wide
    - Important to have backups, which may also be installation media and/or configuration backups
3. **Incident response best practices**
    - A clear policy and incident response plan should be established
    - Scenario playbooks should be created and practiced
    - First response is the organisation's own responsibility, for further analysis, forensics and assistance in recovery, a specialised 3rd party is recommended. Cooperation may be needed as a 3rd party may not have in-depth knowledge of AtoN systems.
    - It is acknowledged that actions to perform incident response may impact AtoN operation and trigger business continuity actions, and thus should be well thought about in advance.
    - A cyber incident should be evaluated by means of a lesson learned exercise, to improve plans and playbooks
4. **The prioritised actions within the continuity plan and for cyber incident response**
    - Risk and impact analysis
    - Planning and preparation
    - Decide on contracting an MSP (Managed Service Provider) / CERT (Computer Emergency Response Team
5. **Means of the reporting and sharing cyber incidents information**
    - It is suggested by the working group that IALA may be facilitator for an ISAC (Information Sharing and Analysis Centre)

Based on the above key points, the group proposed the following topics for future IALA work programme.

- Amend existing IALA recommendation R1009 on Disaster Recovery to include cyber security aspects
- Amend existing IALA guideline G1120 on Disaster Recovery to include cyber security aspects
- Develop a new guideline or recommendation for specifics in cyber incident response and recovery, possibly including crisis management and business continuity management, for AtoN operators and VTS authorities, as operations deviate from generic industry best practices

In addition to these topics, the group developed an informational paper "Inventory of best practices on incident response and recovery and business continuity" (ANNEX E) to all IALA Committees as useful reference for the future work of the Committees and invited the workshop to approve the paper to submit it with the report of the workshop.

The working group discussed that crisis management, especially within a logistics chain, is an important part of cyber incident response, but within the time available, this has not been discussed any further.

Training on both incident response and crisis coordinators may be required. This topic has not been discussed any further within the working group.

It is recommended to address crisis management and training in further committee work.

5.3.2 Introduction

Martijn Ebben opened the working group session by welcoming participants, noting:

- Proposed agenda of the group
- Request to the members to bring the business continuity best practices

The groups was tasked by the following terms of reference from the plenary:

Based on the presentations, comments and questions made at the plenary, WG3 is instructed to;

- Consider the response and guidance during and after a cyberattack event for the different operations and systems impacted;
- Identify business continuity approach and scenarios during and recovering from a cyberattack;
- Identify existing business continuity best practices to be considered within the marine AtoN and VTS operation;
- Identify the prioritised actions within the continuity plan;
- Identify means of the reporting and sharing cyber incidents information for learning;
- If possible, propose topics that may be considered in the future IALA work programme; and
- Submit a report to the plenary by 18 of November 2021.

5.3.3 Discussions

Before discussing each items defined by the terms of reference, the group discussed general matters such as relation and demarcation with other working groups and expectations. Many members expressed their expectations of continuation of aids to navigation service during and after cyber incidents.

Regarding the demarcation with other working groups, some members pointed out that although back up of system or operation such as sending a ship when malfunction of aids to navigation was preventative measures, such measures should be included in the business continuity plan. The members also recognised that detection was between prevention and response and some members pointed out automatic detection/response by system was useful tool for cyber incident. The chair informed that EU laws on cyber security (NIS directive) for important infrastructure, but these did not specify how to detect or response.

Some members mentioned that insurance on cyber incident for ransomware attack of shipping was existed but not covered for aids to navigation service. The chair informed that the US had a policy to minimise ransom payments by government agencies as well as corporations and so gave weight to back up.

The group recognised the importance and usefulness of sharing cyber incident by IALA members but also admitted that such sharing was sometimes difficult and sensitive issue due to secrecy and confidentiality of cyber incident by authorities or organizations.

Then the group discussed the items defined by the terms of reference using a paper submitted by the member as the business continuity best practice and further developed the paper to become an informational document (ANNEX E) from this workshop for the future Committee work.

Some topics were identified that should be part of incident response and recovery but were not discussed in detail. These items are reported for further discussion within the IALA technical committees.

After the discussion, the group agreed the draft working group report with the draft informational document (ANNEX E) and to invite the workshop to;

1. agree the working group report in general and;
2. approve the draft input paper to all IALA Committees.

The Chair thanked all participants for their contribution to the work and closed the working group session.

6. CLOSING SESSION

6.1 Key conclusions

The workshop highlighted the following key conclusions

1. There should be a common terminology understood across an organization, covering not only IT staff but operational, management and technical people as well. E.g., the NIST Framework for Improving Critical Infrastructure Cybersecurity.
2. AtoN including VTS systems are considered critical infrastructure and require the application of Standards implementing security by design, the following reference documentation was recommended:
    - ISO/IEC 27001 Information technology – Security techniques – Information security management systems
    - IEC 62443-4-1 sets out secure product development lifecycle requirements
    - IEC 62443-4-2 specifies technical security requirements for Industrial Automation Control System components
3. There are vulnerabilities in PNT and AIS where IALA could have a key role to play in implementing protection and mitigation measures.
4. Cyber security should be part of the daily business within any organization including operation of AtoN and VTS systems. Raising awareness, implementing procedures, encouraging cyber-secure behaviour and regular cyber-security training should be implemented. Cyber security events and the associated risks should be incorporated in existing business continuity plans.
5. Many legacy systems are still in use that are difficult to maintain in a context of cyber security but may form a suitable back-up to other more advanced systems. This should be recognised in organisational procedures.
6. Assignment of cyber security roles/profiles and associated roles and responsibilities within an organisation is required. This should be recognised in organisational procedures.
7. Cyber security should be embedded into life cycle management of systems.
8. ARM Committee should consider reviewing the IALA risk toolbox to include cyber security.
9. Specific guidance regarding the implementation of cyber security within the AtoN and VTS systems and maritime services is required.
10. The following framework could be a useful reference for best practice in PNT:
    - NISTIR 8323: Foundational PNT Profile: Applying the Cyber security Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services.
11. For the purpose of incident recovery, scenarios for cyber incidents recovery should be developed, in particular for AtoN and VTS systems.
12. A clear incident response plan and policy should be established.
13. First response to cyber incidents is the AtoN and VTS providers' own responsibility. For further analysis, forensics and assistance in recovery, a specialised 3rd party is recommended where the skills are not available in house.
14. Marine AtoN cyber security incidents should be reported and shared to relevant stakeholders.
15. Training on incident response and for crisis coordinators is required within AtoN and VTS system operating organisations.

The Workshop recommended the following key items of further work for IALA:

- A Recommendation for IALA members on how to apply the concepts of security by design to all electronic / connected systems and devices under the IALA remit; and
- To consider how authentication, authorization & encryption can be applied to the systems within the scope of IALA and what are the priorities for these.).
- Amend existing IALA recommendation R1009 on Disaster Recovery to include cyber security aspects
- Amend existing IALA guideline G1120 on Disaster Recovery to include cyber security aspects
- Develop a new guideline and/or recommendation for specifics in cyber incident response and recovery, possibly including crisis management, logistic chain, and business continuity management, for AtoN and VTS operators / providers.
- IALA should consider being a facilitator for an ISAC (Information Sharing and Analysis Centre)

In addition to these topics the WGs have produced further proposals that may be of interest to develop within the IALA committees and that will be referred to during the next work programme:

Working group 1 - Preventative procedural measures and behaviours

Working group 2 – Preventative technical measures

Working group 3 – Incident response and recovery (post operational)

In addition to these topics, WG3 developed an informational paper “Inventory of best practices on incident response and recovery and business continuity” (ANNEX E) as useful reference for the future work of the Committees which is annexed to this report of the workshop:

6.2 Closing remarks

Secretary-General Francis Zachariae made some remarks on the impressive work achieved during the week and chaired by Phil Day and by the working groups chairs and vice chairs. Secretary-General really appreciated the effort and the good contributions coming from the participants. It was also noted that specific work items, workflows and actions were proposed, and Francis Zachariae welcomed those that are to be provided by the IALA secretariat. The consideration of IALA as a a facilitator for an ISAC, is of great interest for the organization. Equally, the action on contributing by a cyber security policy for AtoN and VTS service providers was extremely relevant for the continuity of work in the IALA scope. Secretary-General finally recalled the need to come back at normal face two face business even if the outcome of this workshop becomes essential for the next work program and the IALA members.

The host of the workshop, represented by André Châteauvert from the Canadian Coast Guard and Phil Day expressed their sincere gratitude for all the work done by the (vice) chairs, speakers and experts contributing to the workshop. They also sent their willingness to work in the same room promptly.

ANNEX A LIST OF PARTICIPANTS

Participant	e-mail
Andreas Walderhaug	andreas.walderhaug@knc.kongsberg.com
Emma Stephan	emma.stephan@cerema.fr
Ernest Batty	ernie.b@imisglobal.com
Hideki Noguchi	Hideki.noguchi@gmail.com
Jakob P. Larsen	jpl@bimco.org
Jamie Brennan	jamie.brennan@dfo-mpo.gc.ca
Jim Park	jin.h.park@kriso.re.kr
Jonathan Pritchard	jonathan.pritchard@iictechnologies.com
Luc De Nijs	luc.de.nijs@saabgroup.com
Maarten Berrevoets	Maarten.Berrevoets@minienw.nl
Marcus Krol	marcus.krol@innovative-navigation.de
Martijn Ebben	m.ebben@portofrotterdam.com
Michel Cousquer	michel.cousquer@cerema.fr
Monica Sundklev	Monica.Sundklev@transportstyrelsen.se
MURPHY Helen	helen.murphy@irishlights.ie
Phil Day	phild@nlb.org.uk
Philip Lane	pl@cirm.org
Pierre Mingot	pierre.mingot@cerema.fr
Saito Naoki	n.saito@classnk.or.jp
Sangwon Park	psw6745@kmi.re.kr
Simon Milyard	simon.milyard@trinityhouse.co.uk
Tani Makiko	maki-tani@classnk.or.jp
William Adams	william.c.adams@uscg.mil
Youngsil Lee	lys0113@dongseo.ac.kr
Yunja Yoo	yjyoo@kmi.re.kr
Jillian Carson Jackson	jillian@jcjconsulting.net
Michael Strandberg	mst@dma.dk
Morten Brix Laursen	mbx@dma.dk
Shwu-Jing Chang	sjchang@mail.ntou.edu.tw
Malcolm Nicholson	Malcolm.Nicholson@spx.com
Jens Ohle	jens.ohle@spx.com
Kaisu Heikonen	kaisu.heikonen@ftia.fi
Jeoungkyu Lim	jklim@krs.co.kr
Sanghoon Choi	choish@krs.co.kr
Pierre-Yves Martin	pierre-yves.martin@cerema.fr
Gareth Wimpenny	Gareth.wimpenny@gla-rad.org
Yukimatsu Shunsuke	jcghkokugikaihatsu2-9s8t@mlit.go.jp
Wim Smets	wim.smets@mow.vlaanderen.be
Takeharu Kato	jcghkokugikaihatsu3-3u5j@mlit.go.jp
Anthony Beaupre-Jacques	anthony.beauprejacques@tc.gc.ca
Christopher Jackson	christopher.douglas.jackson@gmail.com

Darren Day	Darren.day@thls.org
Peter Dobson	Peter.Dobson@thls.org
Anna Beckett	Anna.Beckett@nlb.org.uk
Colin Fender	Colin.Fender@nlb.org.uk
Paul Hudson	Paul.Hudson@nlb.org.uk
Guttorm Tomren	guttorm.tomren@kystverket.no
Shivani Seepersad	dawn@seepersad.org
Axel Hahn	axel.hahn@uol.de
Helen Murphy	training@irishlights.ie
Andre Chateauvert	andre.chateauvert@dfo-mpo.gc.ca
Jean-Francois Coutu	jean-francois.coutu@dfo-mpo.gc.ca
Ramesh Pagidipalli	ramesh.pagidipalli@gov.in
Rene Hogendoorn	rene.hogendoorn@saabgroup.com
Dirk Eckhoff	dirk.eckhoff@wsv.bund.de
Stefaan Priem	stefaan.priem@mow.vlaanderen.be
Alan Jacobsen	Alan.Jacobsen@wsv.bund.de
Dongwoo Kang	dwkang@kriso.re.kr
Jose M. Fernandez	jose.fernandez@bastionnage.ca
Sewoong OH	osw@kriso.re.kr
Terry Rambarran	terry.rambarran@yahoo.com
Omar Eriksson	omar.eriksson@iala-aism.org
Jaime Alvarez Velasco	jaime.alvarez@iala-aism.org
Minsu Jeon	minsu.jeon@iala-aism.org
Francis Zachariae	francis.zachariae@iala-aism.org

ANNEX B PROGRAMME FOR THE WEEK

KICK-OFF – Friday, 12th November 2021

Time (UTC)	Activity	
1000 – 1100	**Session 0 – Workshop kick-off**	**Chair: Phil Day**
5 min	Welcome	Phil Day
15 min	Working programme of the week and expectations	Phil Day
15 min	Presentation of input papers	Phil Day
15 min	Working arrangements for the week	Jaime Alvarez / Minsu Jeon
10 min	Q&A	

DAY 1 – Monday, 15th November 2021

Time (UTC)	Activity	
1000 – 1130	**Session 1 – Opening of the Workshop**	**Chair: Phil Day**
5 min	Welcome from IALA	SG / DSG
10 min	Welcome from Canadian Coast Guard	Canadian Coast Guard
5 min	Recalling working programme of the week & expectations	Phil Day, Northern Lighthouse Board
40 min	Presentation 1: Cyber Security in the maritime domain	Jose Fernandez, Bastionnage
15 min	Presentation 2: Cyber Security in other bodies	Jakob P. Larsen, BIMCO
15 min	Presentation 3: Cyber Security in other bodies	Jonathan Pritchard, IHO
10 min	Q&A	
1140 – 1155	**Break**	
1155 – 1255	**Session 2 - Presentations and discussion with expert speakers**	**Chair: Dirk Eckhoff**
15 min	Presentation 1 Cyber security for e-Navigation platforms	Axel Hahn, OFFIS
15 min	Presentation 2 Cyber security for AtoN	Jens Ohle, Sealite
15 min	Presentation 3 Cyber security for VTS	Ernie Batty, IMIS Global Limited
15 min	Q&A	

DAY 2 – Tuesday, 16th November 2021

Time (UTC)	Activity	
1000 – 1115	**Session 3 - Presentations and discussion with expert speakers**	**Chair: Monica Sundklev**
20 min	Preventive measures to ensure Cyber Resilience	Alan Jacobsen, Waterways and Shipping Agency, Germany
20 min	Incident Response and Recovery	Martijn Ebben, Port of Rotterdam
30 min	Cyber Security Risk Management in the maritime domain including the human element	Jose Fernandez, Bastionnage
15 min	Q&A	
1115 – 1130	**Break**	
1130 – 1300	**Session 4 WG Sessions – IALA Guidance and roadmap**	**Chair: Phil Day**
10 min	Establishment of WG	
80 min	Split into working groups: • WG1 Preventative procedural measures and behaviours • WG2 Preventative Technical Measures • WG3 Incident response and recovery - post operational	WG1 chair René Hogendoorn, WG1 vice chairs Stefaan Priem / Jillian Carson-Jackson WG2 chair Philip Lane, WG2 vice chair Jin Hyoung Park WG3 chair Martijn Ebben, WG3 vice chair Hideki Noguchi

DAY 3 – Wednesday, 17th November 2021

Time (UTC)	Activity	
1000 – 1055	**Session 5 WG sessions**	
1055 – 1105	**Break**	
1105 – 1200	**Session 6 WG sessions**	
1200 – 1210	**Break**	
1210 – 1300	**Session 7 WG sessions**	

DAY 4 – Thursday, 18th November 2021

Time (UTC)	Topics	
1000 - 1130	**Session 8 WG sessions**	
1130 – 1145	**Break**	
1145 - 1215	**Session 9 – Report of WG**	**Chair: Phil Day**
10 min	WG1 summary	WG 1 Chair
10 min	WG2 summary	WG 2 Chair
10 min	WG3 summary	WG 3 Chair
1215 – 1300	**Steering committee meeting** *(including WG (vice) chairs and rapporteurs)*	**Chair: Phil Day**
45 min	Develop draft report with findings	IALA Secretariat

DAY 5 – Friday, 19th November 2021

Time (UTC)	Activity	
1100 – 1200	**Session 10 – Documentation review and closing**	**Chair: Phil Day**
45 min	Review findings and draft report	Phil Day
5 min	Closing remarks	SG/DSG
5 min	Closing remarks	Canadian Coast Guard
5 min	Closing of the workshop	Phil Day

ANNEX C TERMS OF REFERENCE OF THE WORKING GROUPS

WG1 - Preventative procedural measures and behaviours

Based on the presentations, comments and questions made at the plenary, WG1 is instructed to;

- Consider that cyberattacks against critical infrastructure are very often mediated through human behaviours or deficiencies in operational or security processes;
- Consider the current level of maturity of cyber security processes and user education in AtoN and VTS operators;
- Identify important industry-wide gaps in organisational security policies and cyber security awareness and priorities for addressing these gaps;
- Identify cyber security management standards that could be adapted and adopted to ensure proper cyber security governance in AtoN and VTS operations;
- Identify which preventive and detection measures should be prioritised;
- Identify desired behaviours, including safety and security culture;
- If possible, propose topics that may be considered in the future IALA work programme; and
- Submit a report to the plenary by 18 of November 2021.

WG 2 – Preventative Technical Measures

Based on the presentations, comments and questions made at the plenary, WG2 is instructed to;

- Consider relevant technologies in operating Marine AtoN, including VTS;
- Identify the most vulnerable systems whose security should be addressed in priority;
- Identify cyberattack scenarios against AtoN, VTS or related systems that would adversely impact maritime operations;
- Identify priority corrective measures on known vulnerable technologies based on risk
- Identify “security by design” approaches that could be adopted in the context of Marine AtoN provision;
- Identify detection technologies and procedures;
- Identify organisations that are dealing with cyber security in the critical infrastructure and/or maritime context; existing standards covering cybersecurity and carry out a gap analysis in the scope of IALA;
- If possible, propose topics that may be considered in the future IALA work programme; and
- Submit a report to the plenary by 18 of November 2021.

WG 3 – Incident response and recovery

Based on the presentations, comments and questions made at the plenary, WG3 is instructed to;

- Consider the response and guidance during and after a cyberattack event for the different operations and systems impacted;
- Identify business continuity approach and scenarios during and recovering from a cyberattack;
- Identify existing business continuity best practices to be considered within the marine AtoN and VTS operation;
- Identify the prioritised actions within the continuity plan;
- Identify means of the reporting and sharing cyber incidents information for learning;
- If possible, propose topics that may be considered in the future IALA work programme; and
- Submit a report to the plenary by 18 of November 2021.

ANNEX D **ABBREVIATIONS**

ADS-B	Automatic Dependent Surveillance Broadcast
AI	Artificial Intelligence
AIS	Automatic Identification System
ANN	Artificial Neural Network
AtoN	Aids to Navigation
ATC	Air Traffic Control
ATTOL	Autonomous Taxiing, Take-Off and Landing
CPDLC	Controller Pilot Datalink
COLREG	Convention on the International Regulations for Preventing Collisions at Sea
DME	Distance Measuring Equipment
DP	Dynamic positioning
EGNOS	European Geostationary Navigation Overlay Service
EICAS	Engine Instrument and Crew Alerting
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
IACS	International Association of Classification Societies
IALA	International Association of marine Aids to Navigation and Lighthouse Authorities
IEC	International Electrotechnical Commission
IFP	Instrument Flight Procedures
IGO	Intergovernmental Organization
IHO	International Hydrographic Organization
ILS	Instrument Landing System
IMO	International Maritime Organization
INAS	International Network for Autonomous Ships
IoT	Internet of Things
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
ISO	International Organization for Standardisation
MASS	Maritime Autonomous Surface Ship
ML	Machine Learning
MSC	Maritime Safety Committee
ODD	Operational Design Domain
OEM	Original Equipment Manufacturers
OEP	Original Equipment Parts
PAP	Policy Advisory Panel
PBN	Performance Based Navigation
PNT	Positioning, Navigation and Timing
NFAS	Norwegian Forum for Autonomous Ships
NGO	Non-governmental organisation
RCC	Remote Control Centre (in MASS context) / Rescue Control Centre (in maritime context)
RSE	Regulatory Scoping Exercise

SESAR	Single European Sky ATM Research
VDES	VHF Data Exchange System
VDL	VHF Data/Digital Link
VTS	Vessel Traffic Services
VTSO	Vessel Traffic Services Operator

ANNEX E INVENTORY OF BEST PRACTICES ON INCIDENT RESPONSE AND RECOVERY AND BUSINESS CONTINUITY

1. Summary

Working group 3 of the IALA workshop on Cyber Security, held virtually on November 15 – 19, 2021, inventoried best practices on business continuity, incident response and incident recovery, which were discussed and edited to be suitable for the domains of AtoN and VTS.

1.1.1 Purpose of the document

This document summarizes the working group's insights and may be used as a starting point for further work in the IALA technical committees.

1.1.2 Related documents

Since the recovery work from cyber incident is similar with other recovery work from natural and other disaster in some degree, the following IALA documents should be referred.

- IALA Recommendation R1009 on Disaster Recovery
- IALA Guideline G1120 on Disaster Recovery

2. Background

The working group was instructed to;

- Consider the response and guidance during and after a cyberattack event for the different operations and systems impacted;
- Identify business continuity approach and scenarios during and recovering from a cyberattack;
- Identify existing business continuity best practices to be considered within the marine AtoN and VTS operation;
- Identify the prioritised actions within the continuity plan;
- Identify means of the reporting and sharing cyber incidents information for learning; and
- If possible, propose topics that may be considered in the future IALA work programme.

2.1 Discussion

The following was discussed during the working group sessions. This text could be used as raw input for further work in the technical committees; it is not to be considered a guideline or recommendation.

2.1.1 Preparation

To prepare for a cyber security incident, it is good to differentiate between.

- Preparations for handling the actual incident; and
- Preparations for handling the consequences of a cyber incident.

Preparations for incident handling should include a risk or impact assessment, which include;

a) Description of risk/incident or potential incident (potential scenarios);
b) Type of data/system involved or at risk
c) Is it sensitive or personal data?
d) Any protections or mitigations already in place?
e) How many systems may be affected?
f) Who is involved (staff, customers, clients, suppliers, general public etc)

g) Extent of risk (physical, safety, reputational, electronic)

h) Impact rating

i) Probability rating

j) Overall risk index (impact x probability)

k) Trigger points on which to escalate to alternative responses in terms of business continuity

Impact assessment should be carried out throughout the process, especially to note if the risk changes as time elapses

It was noted that in assessing risk, the possibility should be considered that malicious activity (a virus, ransomware or hacker) could "hop" through the network. For instance, it may start in an office network via a phishing email, and from there reach the AtoN - or VTS systems.

To continuously perform risk and impact analyses, penetration tests and vulnerability scans of possibly impacted systems may be performed.

- (Automated) vulnerability scanning encompasses a tool that searches for known vulnerabilities or systems
- A penetration test is an audit performed by an ethical hacker that may or may not have additional information, like login credentials, to search for weaknesses.

Additionally, many (national) governmental agencies send regular messages (emails) on newly discovered vulnerabilities, which may be good to subscribe to.

It is important that the plans have full management buy-in and are authorised, sufficiently supported and financed.

In preparation, an organisation may decide to get insurance. The working group noted that an insurance may be;

- An actual insurance for e.g., ransom payment in case of a ransomware incident
- A contract with a managed service provider, including an SLA (Service Level Agreement, ie. Response time etcetera), for assistance in crisis management and incident response and recovery

2.1.2 Incident response best practices

For response to an incident (not business continuity), the following best practices were identified:

- Have a clear policy and incident response plan and ensure that it is accessible without a computer (with contact details, USB thumb drive with plans, forensic tools if required etc). The plan should include required funding for resources and components.
- Test/exercise/practice/simulate and tweak the plan regularly. It is up to the organisation to determine an appropriate interval, so experience and actuality is kept optimal.
- What is defined as an incident – and who categorises it as such? In terms of AtoN it would make sense to define the state as unavailable or unreliable as an incident eligible for the regime described in the plan.
- Classify (potential) incidents – critical, significant, minor, negligible. The classification determines the appropriate action to take. In the context of AtoN, as specified in the previous line, there may be little differentiation. Examples of classification may be found at governmental bodies like the UK National Cyber Security Centre (NCSC).
    - It was noted that a cyber security incident is something that potentially goes wrong as opposed to the ITIL (Information Technology Infrastructure Library) definition of an incident, which states that an incident is something that's gone wrong

- Procedure when there is a breach of Personal Identifying information (GDPR – General Data Protection Regulation - or equivalent) that has mandatory reporting requirements. Names of inland ships are covered under the GDPR as they are usually people's homes.
- Defined incident roles and responsibilities in the response plan – who is responsible for managing the incident, keeping the documentation up to date, making decisions, escalation management, assessing the impact, technical responses, business continuity activities, forensic analysis, communications and so on.
- Clearly defined communications pathway & escalation as part of the response plan
- Scenario playbooks – not only for incident response, also for Business Continuity (see the differentiation between the two)

2.1.2.1 Documentation

One should document all steps as you go along. Most important is to make accurate notes during an incident. A form could be provided as a starting point. Such a form should at least include:

a) Date/time reported

b) Description of the incident

c) How it was discovered/reported and who detected and reported it

d) Status e.g. on-going, recurring, closed

e) Seriousness/severity rating – IALA specific

f) Assessment of affected systems/data

g) Who has been notified of any actions taken

h) Checklist of necessary actions to take/taken, measures, communication and informed people

i) Evaluation and lessons learned

2.1.3 Containment

In containment of a cyber incident, there should be 2 distinct phases;

1. First response – immediate interventive action that can only be performed by the organisation itself
2. Forensic research and thorough investigation and eradication of malicious code, is suggested to be performed by a contracted specialised 3rd party.

Usual steps and considerations in containment include;

- Identify affected systems and what data is compromised
- Collect all information for forensic examination – will probably need expert assistance. Ensure chain of custody is adhered to.
    - In the preparation and planning phase, it is good to ensure that system logging is performed and saved in an orderly manner, to ensure forensics on these can be performed.
- Consider whether the incident response will impact business continuity. An action performed to countermeasure a breach may have more impact on AtoN operations than the actual incident/breach. A decision may be made to leave systems at risk, but operational, for continuity reasons. In technical terms the policy should be defined as "fail open" or "fail close".
- Have a plan relating to scenarios – and decisions regarding disconnecting versus staying online when doing incident response:
- Disconnecting: does not allow you to do a thorough investigation as the problem may disappear/reappear, or be triggered when you disconnect, will alert attacker that you have discovered the breach, shutting down will clear memory which may be needed for forensics,

disconnecting from network may not allow you to find the extent of the compromise. However, a quick response might reduce window of time the attacker or malware has to spread.

- A watch and learn approach may be more likely to tackle the root cause and eradicate, and evidence gathering done properly may allow prosecution. However, this takes time and it will take longer to get back to business as usual.
- In preparation, redundancy should be considered. Not only on a system level, but maybe even on the level of having two completely separated VTS centres (for instance). This may be considered Business Continuity.

Questions to ask:

- What could happen if the breach is not contained as soon as possible?
    - For AtoN operations, this comes down to; are the AtoN operational and reliable or not?
- Is the attack doing severe or immediate damage?
- Is there potential damage and or theft of assets?
- Is it necessary to preserve evidence – and if so, what evidence is needed?
- Is it necessary to avoid alerting attacker?
- Is it necessary to ensure service availability – do we need to invoke Disaster Recovery (DR)?

2.1.4 Incident recovery

Recovery requires eradication of any malicious code and possible backdoors and leftovers.

Take steps to stop breach & start recovering while taking notes simultaneously– steps might include removing malware, changing passwords, identifying gaps and fixing them, adjusting firewall policies, or in the event of major damage, rebuilding servers and restoring from a good backup, The decision to clean up versus rebuild may depend on the severity of the attack and how realistic it is that it can be fully cleaned. Before systems go back online they should be validated from both security and business operations perspective.

Assess if Remote equipment has been affected – might need to get to remote location – ships/helicopters

Root cause of incident leads to information about how best to recover.

In extreme cases, hardware may have been damaged and must be repaired or replaced.

Eradication and recovery is usually a task for experts. Hopefully, no organisation can build the experience to do so by themselves. In AtoN operations however, the used technology may be too specific to handle for (external) experts and a cooperation should be established.

2.1.5 Evaluation

Following an incident, it is important to carry out a Lessons Learned exercise, to be able to learn and improve the plans. Questions to ask during evaluation, and even when drafting the initial response plan include:

1. Was the cyber incident management plan followed?
2. Was the plan adequate? Please give details
3. Should the plan be adapted? Please give details
4. Were there any steps or actions you have taken that might have inhibited the recovery?
5. Could communications have been improved?
    a. In communication, it should be noted that (national) laws may require AtoN organisations to report on cyber incidents if the organisation or its activities are considered vital infrastructure.
6. What corrective actions can be taken to prevent similar incidents in the future?

7. Are there indicators that can be monitored to detect similar incidents more easily in the future
8. What tools or resources were needed to identify/handle the incident?
9. Following from the incident, what tools, training or resources would be recommended to mitigate future cyber security incidents
10. Did the cyber security team have everything they needed to respond to the incident? Were there any hierarchical barriers to taking action?

2.1.6 Best practices on Business Continuity

Business Continuity is an organisation-wide process and includes far more than just cyber security. It should be, however, included in (existing?) business continuity and disaster recovery plans.

Best practices for business continuity after cyber incidents and preparation for them include:

- Ensure that a plan is in place and is tested regularly, i.e. once every year, alternating table top exercises and simulations.
- In AtoN organisations, it is not unusual to have legacy systems in operation. These can both be a high risk and a fall back when computers or automated systems fail.
- Ensure backups and/or virtual machine snapshots are taken regularly and are accessible and tested regularly –depending on system/organisation. Not less than once every 2 years
- Have installation media available and make sure they are useable; for example, to use a CD, a CD-ROM drive is necessary and to program a PLC in a buoy, a laptop with a serial port may be required.
- Immutable (unchangeable) backups/cloud backups and regular validation that they can actually be restored
- Backup schedules and retention – 1 year, monthly, weekly, daily etc. Scale of impact gets greater as you go back. On the other hand, dormant malicious code may have been present for a long time, forcing you to use a very old backup
- Agreed Recovery Point Objective / Recovery Time Objective
    - *Recovery point objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization*
    - *The recovery time objective (RTO) is the amount of real time a business has to restore its processes at an acceptable service level after a disaster to avoid intolerable consequences associated with the disruption.*
- Services in place we can fail over to/who can assist for business continuity

The working group would like to point out that Disaster Recovery differs from Business Continuity. Disaster Recovery is considered to be the IT part of AtoN operations within the overall Business Continuity process.

2.1.7 Priorities in incident response and business continuity

To address incident response and business continuity, the working group identified the following priorities, as a starting point:

1. Risk/impact assessment
    a. Where are the greatest risks
    b. What systems may be most impacted by a cyber incident?
        i. Component level
        ii. (Inter)connected systems
        iii. Consider the human element (carried by a human on a laptop or USB thumb drive

2. Planning / Preparation
    a. Organisational
    b. Continuity plan
    c. Material / contracts / backup systems
    d. Policy: shut down or leave running while at risk
3. Decide on contracting a managed service provider (CERT: Computer Emergency Response Team)
    a. What will you need to do yourself and what can be outsourced?
    b. CERT = Computer – would that be applicable for AtoN? Find the right 3rd party

2.1.8 Means of reporting and sharing cyber incidents

A usual means of sharing information on cyber risk and incidents is to establish an ISAC (Information Sharing and Analysis Centre). This usually is a group of representatives of various companies and organisations that have gained mutual trust and have signed an agreement how to handle sensitive information. They come together, either physically or virtually on a regular basis to discuss actual events, best practices, threats and incidents. Information is not shared outside the ISAC, but may be used, in an anonymised way, to improve the cyber resilience of the participants' organisations.

It is suggested by the working group that IALA may be a facilitator for such an ISAC for IALA members.

There is also technical cooperation. Basically, security systems from different organisations can be interconnected in such a way that if a breach is detected in one organisation, digital signatures may be shared for detection or blocking by the firewall or intrusion prevention system of another organisation.

In sharing sensitive or confidential information, either electronically or verbally, a common practice is to use the Traffic Light Protocol (TLP) for an indication on how to handle the shared information. For information on the TLP, look at https://www.cisa.gov/tlp