Questions	Réponses
Bonjour, comment choisir des équipements souverains quand une majorité des acteurs sont Russes, Americains ou Israeliens ? Dans le cadre de la LPM, il a fallu attendre 3 ans pour avoir des sondes de détection estampillées par l'ANSSI. Merci	
Faites-vous des exercices avec des opérateurs locaux par exemple la CIM ?	ELENGY n'effectue pas d'exercice de ce genre portant sur la cybersécurité.
Peut-il y avoir un risque de cyber attaque via les connexions entre le terminal et les méthaniers via la prise ESD ?	L'ESD fait l'objet d'un simple échange d'information binaire (tout ou rien) entre le terminal méthanier et le navire. Ce type de media et d'échange ne permet pas de véhiculer d'attaque cybersécurité entre l'un et l'autre.
Le sujet de la dronisation adresse clairement la problématique du C2 (Command & Control) et de la résilience. L'autonomisation apporte des vulnérabilités technologiques. Comment envisagez-vous l'entraînement des organisations pour fonctionner sans ces moyens en cas d'attaque ?	
L'OMI prévoit la mise en oeuvre de la Software Quality Assurance (SQA) dans l'e-navigation. Mais la SQA est également une notion récente dans le maritime comme la cybersûreté. Les entreprises et opérateurs ont-ils pris en compte l'importance de la SQA? Car on risque autant un plantage informatique qu'une cyber-attaque.	
Est-ce prudent d'utiliser un système informatique Windows? Pourquoi ne pas utiliser Linux pour les système informatiques des navires?	
Un navire "connecté" pourra-t-il toujours naviguer même si l'IT/OT deviennent inopérant ?	
Les CERT et RSSI des banques partagent des informations de cybersécurité depuis plusieurs années déjà. Y-a-t-il des groupes de travail déjà existants dans le secteur maritime ?	

Bonjour, je voudrais savoir si par exemple pour le port du havre les équipements de transport (APM-Autonomous Prime Mover, grues ou autres) sont équipés pour résister aux attaques Cyber et s'ils ont été testés contre cela ?	Il n'y a pas d'engin de quai téléopéré sur le port du Havre. Je me renseigne auprès des exploitants de terminaux conteneurs pour ce qui est des échanges informatiques entre les engins et les centres opérationnels pour ce qui concerne la télémaintenance.
De quel pays viennent les attaques type Rançongiciels?	
Est ce que les navires participant au contrôle naval volontaire font des reportings sur du brouillage GPS ou spotting AIS? comment est donné l'information aux autres navires?	
Y a il un besoin de formation des gens de mer type TIS avec une durée de validité?	
Bonjour Y-a-t'il des approches (et normes etc) différentes entre cyber-protection maritime et cyber-protection "terrestre" ? Avec éventuelles difficultés à rendre compatibles ? Questionnements auxquels doivent être confrontés les ports et terminaux. Merci	
Est-ce que l'IMO 2021 est plus contraingnante que l'OIV/OSE ?	
Question pour Brittany Ferries : comment pensez-vous pouvoir intégrer la cybersécurité pour des navires dont la durée de vie est de plusieurs dizaines d'années ?	
Question pour le port du Havre : avez-vous eu des échanges en termes de retour d'expérience avec les ports de San Diego ou Barcelone qui ont été victimes d'attaques ?	Les ports d'Anvers, Rotterdam, Hambourg et Le Havre ont constitué un embryon d'ISAC portuaire, mais les ports méditéranéens n'en font pas partie. Il n'y a pas eu d'échange direct relatif à ces attaques avec le port du Havre. L'incident de Barcelonne a cependant du être emonté vers l'ENISA. Il existe également un ISAC Maritime sous couvert de l'association des gardes côtes européens. Considérant l'organisation de la sécurité maritime auxs USA et en Espagne, il est possible que ces incidents aient été traités dans ce cadre.

Question pour Elengy : quels ont été les apports des entraînements cyber pour vous ? Sont-ils systématiques ?	Ces entrainements et exercices permettent de vérifier la connaissance et l'usage des bonnes pratiques et des procédures, de les rappeler le cas échéants et de vérifier la bonne description de notre organisation et des contacts pour la gestion de ce genre d'incidents. Nous pouvons alors si besoin est corriger et améliorer nos processus et nos outils sur la base de REX. Des tests d'intrusions par exemple ("pentests") sont un excellent moyen de relever et corriger d'éventuelles vulnérabiltiés sur notre SI. Enfin, les exercices d'incidents ou de crises sont aussi un bon moyen de vérifier notre réactivité et notre résilience face à ce type d'incident.
Question pour tous : est-ce que vous ressentez une amélioration dans la sensibilisation de vos personnels aux questions de la cybersécurité ?	Pour ce qui concerne la Capitainerie du port du Havre, nous sensibilisons le personnel régulièrement et mettons en œuvre des procédures pour détecter les annomalies de fonctionnement de nos SI opérationels, Nous avons également une procédure pour informer l'ANSI des anomalies détectées.
Question pour tous : vous avez tous été l'objets d'entraînements : est-ce que vous ressentez une réelle plus-value à ce type d'action par rapport à des actions plus traditionnelles de sensibilisation ?	Un exercice majeur a été réalisé au Havre, en lien avec l'ANSI. Le retex montre une orientation beaucoup plus marquée sur la continuité d'activité que sur l'anticipation. Les entrainements devraient cibler la détection des anomalies et la réaction immédiate pour limiter l'impact. Les exercices auxquels j'ai pu participer ou qui m'ont été rapportés restent essentiellement orientés sur la résilience et la communication.
Question pour tous : quelle est votre vision sur la création du futur Maritime CERT annoncée tout à l'heure ? Le voyez-vous comme une réelle plus-value ?	

Question pour @BureauVeritas : comment réaliser une cartographie à bord de navires si complexes si elle n'a pas été réalisée à l'origine ?	BV a développé une méthode fondée sur sa règle NR 659. On commence par inventorier les systèmes à bord, puis les interconnexions entre les systèmes. Nous appliquons un Criticality Assessment de manière à qualifier les systèmes selon trois niveaux. Ce niveau détermine ensuite le niveau de détail requis dans l'inventaire. Nous pouvons ainsi regarder, pour chaque système, les équipements le constituant et les connexions entre ces équipements. Ou nous intéresser à la cartographie des connexions entre le bord et la terre. C'est effectivement un travail qui exige du temps et de l'investissement, côté BV bien entendu, mais aussi côté armateur pour la collecte des informations. En contrepartie, les armateurs se montrent particulièrement satisfaits à l'issue de pouvoir disposer d'une architecture IT/OT claire de leur navire, qui bénéficie directement aux départements informatiques chargés de la maintenance des équipments, de leur mise à jour et de leur maintien en condition de sécurité. Bien entendu cet ensemble est par ailleurs nécessaire à la mise en oeuvre d'un management efficace du risque cyber, comme l'exige l'OMI.
Question pour @BureauVeritas : faut-il s'attendre à une réglementation plus précise de la part de l'OMI ou l'organisme va-t-il se reposer totalement sur les sociétés de classification ?	Il n'est pas connu de projet de spécification détaillée de la part de l'OMI. Il faut probablement compter sur des exigences plus larges dans les années à venir de la part de l'OMI notamment pour les équipments connectés à terre ou la construction neuve. Le BIMCO et l'IACS vont dans ce sens. Quant à la résolution actuelle, même si la DAM a reconnu que la notation de classe "CYBER MANAGED" délivrée par BV répond aux exigences OMI 2021 en termes de management du risque cyber et sera considérée comme telle par les auditeurs ISM, ces derniers conserveront évidemment leur indépendance une fois à bord et seront libres de formuler leurs appréciations. La DAM devrait bientôt éditer un guide dédié CYBER à l'attention des auditeurs ISM, comme elle l'a fait cet été au profilt d'Armateurs de France. Par ailleurs, il est probable que les assurances imposent leurs règles. Un travail avec elles doit être mené c'est ce que préconnise le C2M2 avec un étroite collaboration avec le cabinet BESSE.

Quel est le coût approximatif d'une classification cyber ?	Le coût est bien entendu lié à la complexité de l'armement du navire. Sur une flotte, une homogénéité des équipementiers IT ou OT garantit des gains financiers non négligeables.
Question pour M. Kermarrec : est-ce que les recherches réalisées par la chaire ont des impacts positifs réels pour les navires au quotidien ? Ou s'agit-il uniquement de recherche formelle ?	
Question pour M. Kermarrec et Bureau Veritas : quid de la cybersécurité des navires autonomes et des drones ?	Pour BV, le document NI 641 (Guideline MASS) fait référence à la NR 659 "Rules on Cyber Security for the Classification of Marine Units" et appelle notamment une vérification de type Cyber Secure pour les navires autonomes. La règle NR 659 est également applicable pour les drones.
Les industries qui utilisent l'hyperconexion ont toute été submergé par les vagues d'attaques. N'avez vous pas peur que le navire connecté devienne plus fragile.	
l'IA c'est bien mais il faut beaucoup de données diverses pour que cela soit opérationnel. Nous appliquons cette approche depuis plusieurs années dans notre centre de recherche. Notre problématique est que les sociétés ne veulent/peuvent pas comuniquer leur donné pour des raisons de secrets industriel/procole/législation.... Est il prévut de mettre a disposition des datasets aux centre de recherche?	C'est une des problématique abordée au sein du Centre de coordination de la cybersécurité maritime sur le tiers de confiance
Les méthodes et outils d'analyse des risques sont ils transverses à tous les secteurs ou sont-ils spécialisés par secteur?	Un des objectifs d'une étude puis du développement d'un POC (proof of concept) pourrait être rapidement lancé au sein du comité analyse des risques du C2M2 (Conseil .
Bonjour, y a-t-il une différence de responsabilité cybersécurité entre Armateur et propriétaire du navire ?	
Bonjour Mohammed, pouvez-vous détailler la réglementation applicable que vous avez mentionnée ? Merci	Nous avons nos propres politiques internes. Nous sommes également soumis à certaines législations en matière de cybersécurité sur lesquelles il ne m'est pas permis de m'étendre pour des raisons de confidentialité.
Avez vous déjà relevé des attaques sur les systèmes de bord ? quelles sont les cibles, on a parlé du spoofing AIS; quid des systemes de navigation ou de contrôle des navires ?	

Madame Despoulains bonjour de Portsmouth. y a t'il des dynamiques de coopérations Franco-Britanniques sur les questions de cyberscurité? Merci	De premiers rapprochements ont été effectués avec le M-CERT britanique
Bonjour, Si une réglementation se met en place, y a t-il des mesures de sensibilisation à la cybersécurité qui sont ou seront mises en place pour les acteurs du secteur ?	Aujourd'hui certains acteurs ont mis en place des formations de base et des sensibilisations (le GPMM de Marseille par exemple). L'un des objectifs du centre de coordination cybersécurité maritime est de proposer dans ses offres de services une offre globale, à bas coût qui puisse être évolutive et adaptée au secteur.
L'Information Géographique représente plus de 85% des données des serveurs.Quelles sont les menaces portant sur les données géospatiales (spoofing AIS, suivi de conteneurs, cartographie embarquée, ...)? Quels sont les modes opérateurs de ces "geodata attacks"?	Une fiche de synthèse a été faite sur le rique de spoofing AIS et GNSS par le France au sein du forum des garde-côtes. Un projet de contre spoofing et de sécurisation de l'AIS a été inité par le MINARM et pourrait être décliné à une plus grande échelle pour des navires civils.
L'Information Géographique représente plus de 85% des données des serveurs. Quelles sont les menaces portant sur les données géospatiales (spoofing AIS, suivi de conteneurs, cartographie embarquée, BIM management des infrastructures portuaires ...)? Quels sont les modes opérateurs de ces "geodata attacks"?	
Le domaine maritime est par définition international. La France se met en ordre de marche, mais quid de l'évolution de la reglementation internationale, qui a jusqu'à présent, dans ce domaine, plutôt eu tendance a tout tirer vers le bas	Les règlementations internationales s'établissent à l'OMI et sont effectivement tirées par le bas en raison d'une forte concurrence par les pavillons de complaisance et le fait que les armateurs choisissent d'y inscrire leurs navires. La France via le C2M2 (conseil de la cybersécurité pour le monde maritime) regroupe l'ensemble des acteurs maritimes. Des propositions sont faites à l'OMI mais elles ne peuvent se faire que si déjà l'UE adopte une position semblable. Les ports sont au centre de ces problématiques car c'est eux qui, in-fine réussiront à faire imposer une inversion de la spirale.