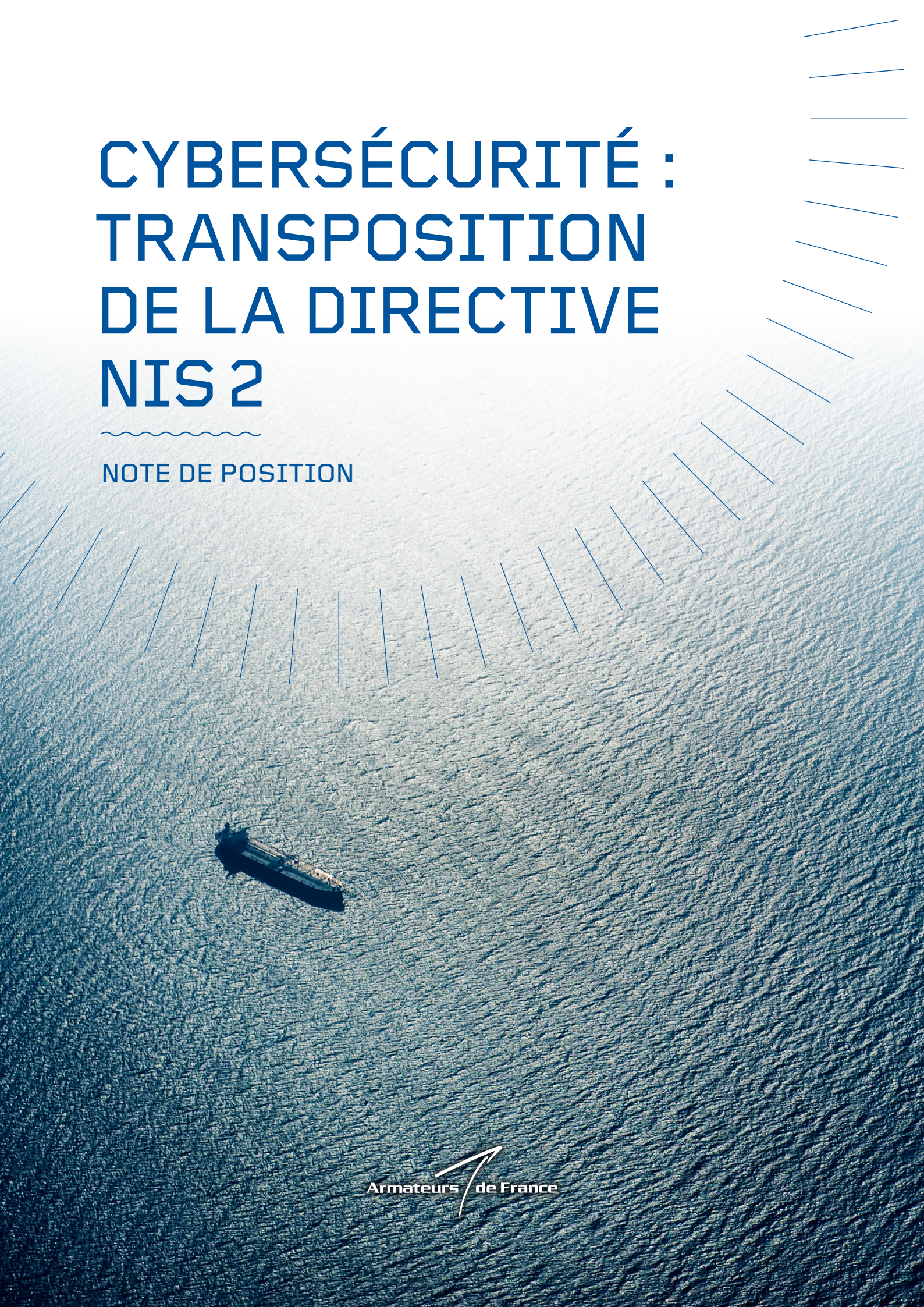
CYBERSÉCURITÉ : TRANSPOSITION DE LA DIRECTIVE NIS 2

NOTE DE POSITION



Armateurs de France

À RETENIR

Les **armateurs français agissent proactivement pour renforcer leur cybersécurité**, par des investissements croissants ainsi que la mise en œuvre et la mutualisation des bonnes pratiques (veille sur les cybermenaces, hygiène informatique, sensibilisation, etc.).

La mise en œuvre de la Directive NIS2 doit permettre de **dégager un avantage compétitif et non conduire à un déficit de compétitivité** des armateurs européens. Pour cela les spécificités du secteur maritime devraient être prises en compte dans le cadre de la transposition, qui doit également **limiter la surcharge administrative** pour les entreprises. Un accompagnement devrait être proposé aux entreprises par l'ANSSI.

Une **application homogène de la Directive NIS2 entre États membres de l'UE** doit pouvoir être garantie, et contrôlée.

Bien que les navires soient exclus du champ d'application de la Directive NIS 2, **il est essentiel que des clarifications soit proposées en ce qui concerne l'articulation de la réglementation européenne avec les autres réglementations dans le secteur maritime, en particulier celles de l'OMI**.

La transposition de la Directive NIS 2 devrait s'appuyer sur une **approche particularisée de l'application de la réglementation** concernant les relations avec les prestataires et les systèmes d'information concernés, les ressources anciennes et la conduite des audits.

Une **progressivité dans l'entrée en vigueur des mesures, des contrôles et des sanctions** devrait être introduite dans le cadre d'une phase transitoire.

CONTEXTE

DES ATTAQUES EN FORTE AUGMENTATION CONTRE LE SECTEUR MARITIME

Depuis plusieurs années, le secteur maritime et portuaire est la cible d'un nombre croissant de cyberattaques (en 2022 une augmentation de 21% par rapport à 2021, et de 135% par rapport à 2020[1]). Au sein du secteur maritime, les ports et les armateurs sont les principaux acteurs ciblés par les attaques au moyen de rançongiciels ou par hameçonnage, avec des cas très hétérogènes selon leur taille, leur niveau de maturité et leur pays d'établissement. Ces attaques ont pour conséquences des atteintes à la disponibilité des services maritimes et à l'intégrité des infrastructures, à terre, comme à bord (interruption de la réservation du fret, perte de contrôle de systèmes essentiels au fonctionnement des navires ou des terminaux portuaires, perturbation des systèmes d'informations, etc.[2]), avec des impacts économiques, réputationnels et des risques en matière de sécurité et de prévention des pollutions de l'environnement marin.

Dans ce contexte, renforcer la cybersécurité du secteur maritime est un enjeu de souveraineté, pour assurer la protection d'infrastructures et de travailleurs essentiels au fonctionnement de l'économie mondialisée. Cette dynamique s'appuie en France sur l'établissement d'une gouvernance sectorielle, avec la création du Conseil Cyber du Monde Maritime (C2M2) et la mise en place de structures et d'outils pour mutualiser les efforts en matière d'identification des menaces, de veille, de réponse en cas d'incident et de partage de bonnes pratiques, avec la création de l'association France Cyber Maritime et la mise en service de son M-CERT[3].

Armateurs de France soutient et contribue à ces démarches sectorielles et les compagnies maritimes français agissent de manière proactive pour renforcer leur cybersécurité, en investissant, en s'organisant et en s'appuyant sur un certain nombre de publications et guides de bonnes pratiques comme celui publié par l'ANSSI et la DGAMPA[4].

UN CADRE JURIDIQUE EN CONSTANTE ÉVOLUTION

Les exigences réglementaires applicables en matière de cybersécurité aux compagnies maritimes font l'objet d'un renforcement continu, aux niveaux national, européen et international. La Directive (UE) n°2016/1148, sur la sécurité des réseaux et des systèmes d'information, dite Directive NIS, a permis l'identification d'un nombre réduit d'opérateurs de services essentiels (OSE) et le renforcement de leur protection contre les menaces cyber. Certains acteurs du transport maritime figurent parmi ces entités[5] et doivent depuis 2016 mettre en œuvre des mesures pour se protéger contre les cyber-risques.

Pour répondre à la montée des menaces cyber, l'adoption de la Directive (UE) n°2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite Directive NIS2, doit conduire à un renforcement conséquent de la cybersécurité des secteurs stratégiques européens parmi lesquels celui des transports par voie maritime regroupant les compagnies maritimes et les ports, considéré comme « hautement critique ». Le dispositif beaucoup plus englobant que celui de la Directive NIS, introduit une logique de « cybersécurité de masse » dans les différents secteurs ciblés.

1- France Cyber Maritime, Panorama de la menace cyber maritime (2022).
2- Bessé, Le secteur maritime et portuaire face au risque cyber (2021).
3- Maritime Computer Emergency Response Team.
4- ANSSI/DGAMPA, Guide de bonnes pratiques de sécurité informatique à bord des navires (2016).
5- En France, 3 compagnies maritimes ont été désignés OSE.

ENJEUX ET IMPACTS POUR LES ARMATEURS

UN ÉLARGISSEMENT DU PÉRIMÈTRE DES ENTITÉS VISÉES AUX COMPAGNIES DE TAILLE MOYENNE

Un grand nombre d'acteurs désignés comme « entités essentielles ou importantes », dans un nombre élargi de secteurs (avec par exemple l'inclusion du secteur de la construction navale), sera désormais soumis aux obligations introduites par la Directive NIS 2. La notion d'OSE sera supprimée et remplacée par un mécanisme de seuil[6]. Les exigences de la Directive NIS 2 ont vocation à s'appliquer à l'ensemble des réseaux et systèmes d'information des armateurs[7].

Les exigences seront étendues à l'ensemble de la chaîne de valeur des secteurs ciblés. Seront donc également concernés les prestataires de services de confiance qualifiés, les fournisseurs de réseaux publics de communication, et les Administrations des États membres. Une mécanique de désignation par les États membres permettra également d'intégrer dans le périmètre des entités sur la base de critères spécifiques (monopole, risque environnemental, etc.).

Armateurs de France, organisation qui représente 54 compagnies maritimes, estime[8] que près de 70 % des armateurs français adhérents de l'organisation pourraient être soumis aux nouvelles exigences, soit en tant qu'EI (plus de 50 %), soit en tant qu'EE. L'élargissement considérable du nombre d'entités concernées devrait faire l'objet d'une sensibilisation accrue et d'un accompagnement des opérateurs par l'ANSSI.

DES EXIGENCES ET DES CONTRÔLES RENFORCÉS POUR UN INVESTISSEMENT SOUTENU DES ARMATEURS

Les EE et les EI devront mettre en œuvre des mesures techniques, opérationnelles et organisationnelles pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information et notifier les incidents. Une logique de proportionnalité concernant ces exigences, la supervision du respect de celles-ci et les sanctions en cas de non-conformité sera introduite (dont les modalités seront précisées dans le cadre de la transposition).

La mise en conformité avec la Directive NIS 2, aura un coût significatif pour les armateurs avec la nécessité de recruter de nouvelles ressources humaines[9] ou de faire appel à des expertises externes, et générera une surcharge administrative importante. Cet impact économique sera variable selon la taille et le niveau de maturité des compagnies (80 % des adhérents d'Armateurs de France sont des TPE ou des PME). Elle aura ainsi un impact sur la compétitivité des compagnies maritimes européennes, vis-à-vis de leurs concurrentes étrangères.

UN CALENDRIER DE TRANSPOSITION ET DE MISE EN CONFORMITÉ RESSERRÉ

Adopté fin 2022, la Directive NIS 2 est en cours de transposition par les États membres, jusqu'au plus tard à octobre 2024. Dans le cadre de la transposition des consultations ont été conduites par l'ANSSI sur différents aspects : le périmètre des entités régulées, les relations entre l'Agence et les futures entités régulées, et le contenu des exigences auxquelles elles seront soumises. Armateurs de France y a contribué en tant qu'organisation représentative des entreprises de transport et de services maritimes.

L'échéance d'entrée en vigueur du texte est donc courte, et à l'issue des délais de mise en conformité devraient être aménagés pour laisser aux opérateurs suffisamment de temps pour réaliser leur mise en conformité dans les meilleures conditions. Durant ce délai de transposition, il est également nécessaire que les spécificités du secteur maritime puissent être identifiées et fassent l'objet d'une approche particularisée si nécessaire.

6- Les entités concernées sont les entreprises qui dépassent les plafonds applicables aux moyennes entreprises tels que définis par la recommandation de la commission 2003/361/EC : Entité importante (EI) : entreprise dont le nombre d'employés est supérieur ou égal à 50 OU dont le chiffre d'affaires annuel atteint au minimum 10 millions d'euros ; Entité essentielle (EE) : entreprise dont le nombre d'employés est supérieur ou égal à 250 personnes ET dont le chiffre d'affaires annuel ou le total du bilan annuel excède 50 millions d'euros.

7- À l'exception des navires, conformément à l'annexe I de la Directive.

8- Statistiques établies sur la base des déclarations de chiffre d'affaires des compagnies adhérentes et des données connues au niveau de la branche concernant le nombre d'employés des armateurs français.

9- Le recrutement d'experts cyber est coûteux et difficile car ces ressources sont très recherchées.

POSITION D'ARMATEURS DE FRANCE

APPROCHE GÉNÉRALE

Les armateurs français soutiennent le renforcement des exigences cyber pour faire face à l'augmentation des cybermenaces visant le secteur maritime et plus largement l'ensemble de l'économie et des infrastructures stratégiques.

Armateurs de France appelle toutefois à une vigilance concernant les impacts économiques (investissements, recrutements, etc.) et organisationnels (surcharge administrative, etc.) ainsi que sur les risques d'introduction de distorsions de concurrence avec la nouvelle réglementation pour les compagnies européennes, exposées à une concurrence internationale. La mise en œuvre de la Directive NIS 2 doit permettre de dégager un avantage compétitif et non conduire à un déficit de compétitivité des armateurs européens.

Une application homogène de la Directive NIS 2 au niveau européen doit pouvoir être garantie, et contrôlée. La transposition de la réglementation doit limiter la surcharge administrative pour les entreprises.

La mise en conformité des entreprises avec les exigences de la Directive NIS 2 devrait faire l'objet d'un accompagnement de la part de l'ANSSI et un certain nombre de points pourraient être précisés pour garantir la sécurité juridique des opérateurs. Les efforts de renforcement de la cybersécurité des entités régulées devraient tout particulièrement être soutenus, y compris financièrement.

PÉRIMÈTRE DES ENTITÉS RÉGULÉES

Armateurs de France et ses adhérents soutiennent les positions suivantes :

- **Extension des exigences aux relations avec les prestataires :** bien que l'introduction des nouvelles exigences soit tout à fait nécessaire, il ne faudrait pas qu'un même niveau d'exigence soit imposé à l'ensemble des prestataires. Une approche particularisée en fonction du type et de la criticité des prestataires devrait être soutenue. Également, l'application des exigences de la Directive NIS 2 aux relations avec des prestaires étrangers à l'UE pourrait être précisée (notamment en ce qui concerne les contrats via des filiales à l'étranger, particulièrement courants dans le secteur maritime). Les opérateurs s'interrogent également sur les efforts de communication et de sensibilisation de l'UE à l'égard des prestataires étrangers.

- **Périmètre d'application aux systèmes d'information :** avec la Directive NIS 2 la notion de système d'information essentiel disparaît. Antérieurement, avec la Directive NIS cette catégorie permettait à l'opérateur de procéder par déclaration à la désignation des systèmes couverts par les exigences réglementaires en fonction des domaines métiers jugés essentiels. Une approche particularisée en fonction du type et de la criticité des systèmes d'information devrait être soutenue.

- **Délai de mise en conformité :** la mise en conformité des entreprises devrait pouvoir bénéficier d'une phase transitoire suffisamment longue avant contrôle et éventuelle sanction une fois la transposition de la Directive NIS 2 effective en droit français. Un délai différencié de 3 mois à 3 ans selon les mesures, et fondé sur le retour d'expérience des OSE, devrait être soutenu.

- **Articulation avec les normes de l'Organisation maritime internationale (OMI)** : bien que les navires soient exclus du champ d'application de la Directive NIS 2, il est essentiel que des clarifications soit proposées en ce qui concerne l'articulation de la réglementation européenne avec les autres réglementations concernant la cybersécurité dans le secteur maritime, en particulier les exigences au niveau international de la résolution MSC.428(98) adoptée par l'OMI. En effet, les armateurs gèrent des SI hétérogènes, avec une partie à bord des navires et une partie à terre. Or la Directive NIS 2 ne s'appliquera qu'à la terre, ce qui pourrait accroître cette hétérogénéité.

RELATIONS ENTRE L'ANSSI ET LES ENTITÉS RÉGULÉES

Armateurs de France et ses adhérents soutiennent :

- **La désignation par les entités régulées de points de contact à l'ANSSI :** 2 pour les EE (RSSI[10] et point de contact en cas d'alerte ou d'incident) et 1 pour les EI (seulement un point de contact en cas d'alerte ou d'incident). La réactivité exigible de ces points de contact devrait tenir compte des ressources disponibles et des astreintes mises en œuvre (jusqu'à 24h de délai en fonction des sociétés).

- **L'utilisation d'outils de partage volontaire d'informations** sur les incidents, les vulnérabilités, les cybermenaces, les incidents évités notifiés, en particulier le M-CERT de France Cyber Maritime. Un tel outil doit être simple et peu coûteux, en particulier pour les PME.

- **La création d'une plateforme numérique et d'une application mobile par l'ANSSI pour permettre la dématérialisation des démarches administratives**. Celle-ci devrait être la plus simple, accessible et générique possible, avec des accès sécurisés.

- **La mise en œuvre d'un mécanisme de certification** des EE et EI qui pourrait être un facteur de compétitivité pour eux dans le cadre de certains appels d'offre vis-à-vis de compagnies maritimes étrangères (notamment dans le cadre de certains marchés publics).

L'organisation appelle à une vigilance concernant :

- **Le délai de signalement des incidents :** il ne devrait pas être trop court car évaluer un incident peut prendre du temps. Certaines compagnies manquent de ressources. Un délai de 48h pourrait être préférable ou une simple notification plutôt qu'un signalement précis et circonstancié. Une majorité d'entités régulées dans le secteur maritime est en mesure de déclarer les « incidents évités » mais pas la totalité. Une telle démarche ne devrait donc pas être rendue obligatoire.

10- Responsable de la sécurité des systèmes d'information.

- **Les informations à communiquer à l'ANSSI par les entités régulées :** il est nécessaire de limiter les exigences de fournitures de données déjà publiques, par les entités régulées pour réduire la surcharge administrative. Il est également suggéré de préciser plus spécifiquement le lieu d'hébergement des systèmes soumis à la Directive (cloud US / UE / Chine / datacenters, etc.). Concernant les informations relatives au chiffre d'affaires il serait préférable de répertorier les entreprises par tranches.

MESURES DE GESTION DES RISQUES CYBER

Dans l'établissement du référentiel de règles de cybersécurité NIS 2 au niveau national, Armateurs de France et ses adhérents sont tout particulièrement attentifs à :

- **La possibilité de proposer des moyens alternatifs de mise en conformité** pour atteindre les objectifs de la réglementation, dans une approche particularisée (notamment concernant les SI, les relations avec les prestataires, les ressources anciennes – systèmes legacy - et la conduite des audits) ;

- **La prise en compte des spécificités liées à l'usage du Cloud** (notamment concernant les règles en matière de cloisonnement) ;

- **La caractérisation claire et formelle de la notion de criticité** et de la notion de système ;

- **Les délais d'installation des correctifs** ainsi que les modalités et périodicité de configuration des ressources ;

- **Les règles applicables à l'accès aux locaux techniques et aux serveurs** (notamment en articulation avec les exigences de l'OMI en matière de sûreté) ;

- **La clarification des exigences pour le niveau exécutif de l'entité**, en matière de réaction aux incidents de sécurité, de gestion de crise et de continuité de l'activité.

CONTACT
Pierre-Antoine Rochas, Responsable sécurité-sûreté-ports d'Armateurs de France
pa-rochas@armateursdefrance.org