CYBER CERCLE

10 DÉCEMBRE 2020 en distanciel

RENCONTRES CYBERSÉCURITÉ NORMANDIE

#RCYBERNORMANDIE
#TDFCYBER2020

LE HAVRE port
HAROPA

TOUR DE FRANCE DE LA CYBERSÉCURITÉ 2020

#TDFCyber2020

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS

@CyberCercle
@CyberTerritoire

DOSSIER PARTICIPANT

RCyberNormandie en distanciel 10 DÉCEMBRE 2020

Crédit photo Alain Zimeray

Bénédicte PILLIET
Présidente
CyberCercle

Edito

Le CyberCercle a fait de la sécurité et la confiance numériques des territoires un des axes forts de son action depuis plusieurs années. Dans le prolongement de nos événements « Cyber et Territoires », nous avons ainsi lancé en 2018 le Tour de France de la Cybersécurité.

Aller au contact des acteurs locaux pour promouvoir la sécurité et la confiance numériques afin d'en faire des axes stratégiques, engager des synergies au sein des écosystèmes, des territoires et entre les territoires, susciter des projets fédérateurs, être force de propositions… sont les moteurs de notre action et de notre motivation en région.

Avec la crise sanitaire, le Tour de France de la Cybersécurité s'est bien évidemment réinventé en maintenant deux objectifs majeurs : permettre dans le contexte actuel d'avoir accès à une parole de confiance sur la sécurité numérique ; favoriser les échanges constructifs pour avancer ensemble vers des territoires numériques de confiance, alors même que le recours au numérique est devenu d'autant plus essentiel avec la crise que nous traversons.

Cette étape du Tour de France de la Cybersécurité, qui aurait dû se dérouler en présentiel au Havre, est très particulière.

Face aux enjeux et à la structuration majeure que représente le projet de Smart Port City pour le territoire et l'écosystème havrais, le fil rouge de cette étape s'est naturellement articulé autour de la dimension cybersécurité maritime et portuaire, qui est en outre un autre axe majeur de l'action du CyberCercle depuis 2014.

Comment innover via un numérique de confiance pour transformer les métropoles industrielles et portuaires ? telle est la question à laquelle nous essaierons de répondre tout au long de cette journée à travers table ronde, keynotes, ateliers de travail réunissant des intervenants de grande qualité que je tiens à remercier pour leur mobilisation en ces temps compliqués.

Force est de constater, une fois de plus, que le travail à accomplir pour que nos territoires deviennent des territoires numériques de confiance, pour que des projets comme le Smart Port City irriguent de façon positive l'ensemble de l'écosystème, favorisant le développement économique, la sécurité et des usages sécurisés au service des citoyens, des entreprises, des collectivités, est encore immense. Nous en sommes seulement au début mais nous devons avancer vite, et ensemble.

C'est aussi le sens de cette journée : travailler ensemble.

Je tiens à remercier HAROPA - Port du Havre et son directeur général, Baptiste MAURAND, l'UMEP, et son président, Michel SEGAIN, de leur implication dans l'organisation de cette journée, autour d'un projet au cœur de leurs enjeux.
Merci également à nos partenaires, qui pour certains nous suivent sur l'ensemble du TDFCyber depuis sa création comme le Groupe La Poste, Cybermalveillance.gouv.fr et CERTitude NUMERIQUE, des entreprises comme FORTINET, Avant de Cliquer et SIEMENS qui s'y investissent davantage cette année, le GICAN qui est à nos côtés sur la cybersécurité maritime depuis 2014. Je remercie enfin nos soutiens, ministères, écoles, associations, qui s'associent à cet événement dans cet esprit fédérateur qui est le nôtre.

Rappelons-nous que la confiance et la sécurité numériques demandent un effort individuel mais surtout collectif, une dynamique de gouvernance, un élan allant bien au-delà de la sphère des experts dans laquelle elle est encore trop souvent enfermée.

« *Agir efficacement ensemble pour construire une culture de sécurité numérique partagée au service des acteurs présents sur les territoires », telle est la signature du Tour de France de la Cybersécurité.* »

Cette première édition des Rencontres de la Cybersécurité Normandie, dans sa dimension portuaire, s'inscrit pleinement dans cette dynamique constructive, d'autant plus indispensable pour faire face aux enjeux actuels, qu'ils soient économiques, sécuritaires ou sociétaux.

DOSSIER PARTICIPANT

RCyberNormandie en distanciel 10 DÉCEMBRE 2020

Edito

Baptiste MAURAND
Directeur Général
HAROPA - Port du Havre

Je suis très heureux d'accueillir cette 2ème édition des Rencontres de la CyberSécurité en Normandie, à l'instar de la 1ère édition qui s'était tenue au Havre en 2018.

Organisé par le CyberCercle avec le soutien de HAROPA - Port du Havre et de nombreux partenaires, cet évènement fédérateur associe institutions publiques, associations, collectivités, élus, acteurs privés, universités, qu'ils soient locaux, nationaux ou européens.

La filière maritime fait le constat, comme d'autres filières, d'une augmentation significative du nombre d'incidents Cyber.
Cette année plus encore, nombre d'entreprises, déjà fragilisées par la crise Covid, ont été touchées par des cyber-attaques.

La cybersécurité est donc l'un des sujets majeurs des ports français. C'est peut-être même la priorité pour les ports de commerce, comme Le Havre, qui par définition sont des lieux ouverts pour faciliter tant les flux physiques que numériques. L'interconnexion généralisée des systèmes et des technologies de l'information expose les acteurs portuaires à des menaces cyber de plus en plus importantes.

HAROPA – Port du Havre, a intégré depuis de nombreuses années dans sa stratégie cette dimension avec la volonté de favoriser plus largement la prise en compte du risque cyber sur le territoire. Le volet cyber a, par exemple, été intégré dès le début du programme Le Havre Smart Port City avec pour ambition d'élaborer une plateforme de cybersécurité portuaire, maritime et industrielle de premier plan. Un projet qui s'est concrétisé en 2019 avec la signature d'un accord de partenariat avec AIRBUS, l'UMEP et SOGET. Nous avons également des partenariats en cours avec notre Capitainerie et d'autres services du Port pour permettre de renforcer notre réactivité.

Par ailleurs, la dimension cybersécurité du Havre - et de l'axe Seine en général - doit devenir un élément différentiant pour nos clients/prospects et l'attractivité des offres de services HAROPA. C'est pourquoi, nous nous sommes saisis de ce sujet en priorité, pour être « prêts », prêts à faire face à ces cyber-attaques, de plus en plus nombreuses et de plus en plus destructrices pour nos écosystèmes portuaires comme pour l'organisation de tous les ports français et de leurs places portuaires en général. La préparation et l'anticipation, partie intégrante du risque, est aujourd'hui un argument commercial pour nos clients dans le choix d'un port. Il y a donc nécessité à innover vers un numérique de confiance pour transformer nos territoires, nos activités et surtout rassurer nos clients.

A l'instar de la mobilisation de notre écosystème local autour du projet Smart Port City, c'est ensemble que nous relèverons ce défis et porterons cette thématique de « confiance ».
Nous avons autour de nous des acteurs de référence, des industriels, des universitaires, des professionnels du secteur, des sachants... pour nous apporter toute leur compétence et leur expertise sur les questions de Cybersécurité et qui nous permettent de faire de la France l'un des fers de lance de la défense anti-cybercriminalité.

C'est évidemment pour nous tous un atout majeur pour un enjeu majeur.

8h45 **MOTS DE BIENVENUE**

- **Bénédicte PILLIET**, présidente, CyberCercle
- **Baptiste MAURAND**, directeur général, HAROPA - Port du Havre
- **Michel SEGAIN**, président, Union Maritime et Portuaire

INTERVENTIONS D'OUVERTURE

- **Catherine MORIN-DESAILLY**, sénatrice de la Seine-Maritime, membre de la commission Culture, Education et Communication du Sénat, membre de la commission des Affaires européennes
- **Cornélia FINDEISEN**, directrice générale adjointe en charge du Département Attractivité et Aménagement du Territoire, Communauté Urbaine Le Havre Seine Métropole - représentante de Jean-Baptiste GASTINNE, 1er Vice-président de la Communauté Urbaine Le Havre Seine Métropole en charge du développement économique et du tourisme

9h30 **TABLE RONDE**

Comment un projet d'envergure tel que le Smart Port City contribue au développement d'un territoire numérique de confiance ?

Animateur : **Bénédicte PILLIET**, présidente, CyberCercle

Kris DANARADJOU, directeur général adjoint, HAROPA - Port du Havre
Michel CADIC, délégué ministériel adjoint, Délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité, ministère de l'Intérieur (DPSIS)
Andreas SCHWAB, député européen
Jean-Marie DUMON, délégué général adjoint, GICAN
Bruno BENDER, coordonnateur cyber pour le monde maritime, Comité France Maritime

10h45 **KEYNOTES**

- La sécurité numérique à l'heure du COVID-19 : retour sur l'action de Cybermalveillance.gouv.fr et recommandations

Laurent VERDIER, chargé de mission sensibilisation risque cyber, Cybermalveillance.gouv.fr

- Présentation détaillée de la **plate-forme industrielle, maritime et portuaire** du projet TIGA Smart Port City du Havre

Jérôme BESANCENOT, chef du Service du développement des Systèmes d'Information, HAROPA - Port du Havre

- L'**identité numérique** : comment et pour quoi faire ?

Dr Michel DUBOIS, chef du bureau Expertise, direction de la cybersécurité, Groupe La Poste

- RETEX du **dispositif numérique déployé par HAROPA Port du Havre lors de la crise du COVID-19**

Gildas REUL, responsable du Pôle Sûreté et Continuité d'Activité, HAROPA - Port du Havre

13h00 **FIN DE LA MATINEE**

14h30 **ATELIERS**

Les ateliers durent deux heures et ont pour objectif de permettre aux participants d'échanger, de façon très pratique et opérationnelle. Ils sont placés sous les règles de Chatham House. Des orateurs ouvrent l'atelier par des exposés d'une douzaine de minutes chacun pour poser le cadre puis l'ensemble des participants est invité à s'exprimer, soit pour poser des questions, soit pour apporter un témoignage, un retex ou une vision du sujet. A l'issue, des points forts de ces échanges sont présentés via un compte-rendu sur notre site.

➤ De la sécurisation des infrastructures à la mobilité intelligente, comment combiner cybersécurité et **systèmes automatisés** ?

Philippe GENOUX, délégué général, Association des EXploitants d'Equipements de mesure, de Régulation et d'Automatismes (EXERA)
Fabien MIQUET, Product & Solution Security Officer, Siemens Digital Industries France
Dr Florence LECROQ, maître de Conférences, Université Le Havre Normandie
Colonel Florian MANET, commandant la Section de Recherches de Bretagne, Gendarmerie Nationale

➤ **Innovation** et cybersécurité au service du monde maritime - IoT, IA, Corridor 5G, mobilité intelligente, gestion de la donnée

Yann VACHIAS, directeur général adjoint, Ecole Nationale Supérieure Maritime
William LECAT, directeur de programme Grand Défi automatisation de la cybersécurité, Secrétariat Général pour l'Investissement
Christophe AUBERGER, Evangéliste Cybersécurité, FORTINET France
Cyril CHEDOT, responsable du service Planification de l'aménagement du territoire, HAROPA - Port du Havre
Cyrille BERTELLE, directeur, SFLog - professeur, Université Le Havre Normandie

➤ Comment **sensibiliser en interne** ses collaborateurs aux bonnes pratiques de la sécurité numérique ?

Atelier de Cybermalveillance.gouv.fr animé par Laurent VERDIER, chargé de mission sensibilisation risque cyber, Cybermalveillance.gouv.fr
avec **Carl HERNANDEZ**, co-fondateur, Avant de Cliquer

➤ Quels **métiers** et quelles **formations** de cybersécurité appliqués au maritime ?

Alexandra BIGAS, membre, CEFCYS
Olivier LASMOLES, professeur associé en droit portuaire, chef du département supply chain management et sciences de la décision, EM Normandie
Pedro MERINO-LASO, professeur, Ecole Nationale Supérieure Maritime
Yvon KERMARREC, directeur, Chaire de cyberdéfense des systèmes navals, Ecole Navale
Laurane RAIMONDO, DPO - chargée de cours, CLESID

➤ Quelle **gestion de crise** et quels **enseignements** tirer au niveau du numérique de la **COVID-19**, par les acteurs maritimes du territoire havrais ?

Dr Michel DUBOIS, chef du bureau Expertise, direction de la cybersécurité, Groupe La Poste
Gildas REUL, responsable du Pôle Sûreté et Continuité d'Activité, HAROPA - Port du Havre
Jean-Michel VILLEVAL, délégué Général, SYNERZIP LH
Stéphane FRONCZAK, chef de la cellule CYBERGENDMAR, Gendarmerie Maritime
Julien PREVEL, directeur des Ressources Humaines, membre du Directoire, SOGET

16h30 **FIN DES ATELIERS ET DE LA JOURNÉE**

Les intervenants

RENCONTRES CYBERSÉCURITÉ NORMANDIE

Catherine MORIN-DESAILLY

Sénatrice de la Seine-Maritime, Présidente de la Commission de la Culture, de l'Education et de la Communication

Professeure d'anglais de formation et diplômée en 2007 de l'Institut des Hautes études de l'entreprise, Catherine MORIN-DESAILLY exerce ses premières fonctions politiques en 1995 lorsqu'elle est élue adjointe au maire en charge des affaires scolaires et de la jeunesse à Bois-Guillaume (76). Elle est par la suite adjointe au maire de la ville de Rouen, déléguée à la Culture. Après avoir été élue conseillère régionale de Haute-Normandie, Catherine MORIN-DESAILLY est élue sénatrice de la Seine-Maritime le 26 septembre 2004. Après avoir été Vice-présidente de la Commission des Affaires européennes du Sénat de 2011 à 2014, elle est depuis 2014 Présidente de la Commission de la Culture, de l'Education et de la Communication. Rapporteure du budget média, auteure de plusieurs rapports sur l'audiovisuel public et sur le numérique, elle a également été rapporteure pour avis de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique. Elle a par ailleurs participé plusieurs groupes de travail et à la rédaction de rapports parlementaires, en particulier le rapport sur la gouvernance européenne du numérique : « l'UE, colonie du numérique ? » publié en 2013 et qui a fait l'objet d'un avis politique du Sénat auprès de la Commission Européenne à Bruxelles. Catherine MORIN-DESAILLY a été également à l'initiative de la création d'une mission commune d'information sur le thème « Quels nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet ? ».

Réélue en septembre 2020 sénatrice de la Seine-Maritime, Catherine MORIN-DESAILLY est actuellement membre de la commission des Affaires européennes, membre de la commission de la Culture, de l'Education et de la Communication, Vice-présidente de la délégation sénatoriale à la prospective.

Baptiste MAURAND

Directeur Général
HAROPA - Port du Havre

Diplômé de l'Ecole Nationale des Ponts et Chaussées ainsi que de l'Université de Westminster, Baptiste Maurand, âgé de 38 ans, est spécialiste des politiques de transport.
Il a commencé sa carrière au sein des services de l'Etat en Normandie puis de la Direction Générale des Infrastructures, des Transports et de la Mer (DGITM). Il a notamment développé pour le compte de l'Etat des projets de fret ferroviaire en concession de service entre la France et l'Italie. Il a également été chef du projet Charles de Gaule Express, futur train express reliant l'aéroport de Roissy Charles-de-Gaulle à la Gare de l'Est.
En 2014, Baptiste Maurand a rejoint le cabinet d'Alain Vidalies, Secrétaire d'Etat chargé des Transports, en tant que conseiller technique pour les infrastructures de transport ; il travaille notamment à la coordination de la politique d'investissement routière, ferroviaire et fluviale à l'échelle nationale, ainsi que des grands projets.
En octobre 2016, il a été nommé Directeur Général Adjoint du port du Havre. Dans un contexte de rapprochement avec les ports de Rouen et de Paris au sein du GIE HAROPA, il a été en charge de dossiers stratégiques parmi lesquels la mise en place du programme d'investissements de 600 M€ pour le développement 1er port pour le commerce extérieur de la France, mais également la préparation du Brexit ainsi que le défi de « smart port » pour accompagner la transformation numérique du Havre et des territoires de l'axe Seine.
Baptiste Maurand est Directeur général de HAROPA - Port du Havre depuis avril 2019.

Bénédicte PILLIET

Présidente fondatrice
CyberCercle

Crédit photo Alain

Bénédicte Pilliet est depuis 2011 la Présidente fondatrice du CyberCercle, cercle de réflexion, d'expertise et d'échanges placé sous la dynamique des élus, parlementaires et locaux, qui traite des questions de confiance et de sécurité numériques. Avec deux objectifs majeurs : favoriser la diffusion d'une culture de sécurité numérique et agir au niveau des politiques publiques dans ce champ, aux niveaux national et local.
Bénédicte Pilliet est responsable du séminaire "Politiques publiques de cybersécurité et Relations internationales" au sein du M2 "Politiques de Défense-Sécurité et Relations internationales" à l'Université de Toulouse Capitole 1, et directeur pédagogique du Certificat Sécurité Numérique de l'Université Paris-Dauphine. Elle est chargée de cours à l'Université Catholique de Lyon et à l'Institut Léonard de Vinci, intervient comme experte dans des formations d'entreprises et des colloques.
Diplômée de Sciences Po Paris en 1990, Bénédicte Pilliet a acquis à travers son parcours professionnel une expertise reconnue dans la communication institutionnelle et les Affaires Publiques, sur les sujets de défense, de sécurité nationale et de sécurité numérique.
Elle a rejoint en 2007 la Réserve Citoyenne de l'armée de Terre, puis en 2012 la Réserve Citoyenne de Cyberdéfense où elle sera en charge du rayonnement jusqu'en 2018. Elle est titulaire de la Médaille de la Défense nationale, échelon or, agrafe cyber, et de la Médaille des Services Militaires Volontaires, échelon bronze.
Bénédicte Pilliet est Vice-présidente de l'association Les Amis de la RCC, membre d'honneur du CEFCYS (Club des Femmes de la Cybersécurité), membre fondateur du Cercle K2 et membre du CESIN (Club des Experts de la sécurité de l'information et du numérique).

Michel SEGAIN

Président
Union Maritime et Portuaire

Michel SEGAIN, né en 1954, marié, deux enfants, est titulaire d'un Certificat d'études primaires et d'un Diplôme de comptabilité (Pigier).
C'est en 1968, à l'âge de 14 ans, qu'il débute sa carrière dans le Maritime au sein de la Compagnie des Chargeurs Réunis.
Puis, en 1975, une fois son service militaire fini, il démarre une carrière dans le Transit chez ATT en qualité d'employé de Transit puis chef Adjoint du Service Import.
Il consolide son expérience dans la Commission de Transport dans différentes sociétés et, en 2001, Monsieur SEGAIN décide de créer sa propre société : TRANSIT MEAL.
Son engagement pour le développement du Port du HAVRE l'amène à devenir Administrateur du Syndicat des Transitaires du Havre, puis Vice-Président et Administrateur de l'UMEP.
En 2015, il est élu Président de l'Union Maritime et Portuaire du HAVRE (UMEP : 600 entreprises, 22 000 emplois).
En Mai 2016, il devient Président Fondateur de la Fédération SEINEPORT UNION (Ex FCPAS : 1100 entreprises, 60 000 emplois), la Fédération des Communautés Portuaires de l'Axe Seine.
En Février 2019, il est élu Président de l'Union Maritime et Portuaire de France (UMPF : 1 600 entreprises, 80 000 salariés) dont les Membres sont des Unions Maritimes et/ou Portuaires de Métropole et d'Outre-Mer.
En Juillet 2020, il est reconduit par ses pairs dans ses fonctions nationales.

Les intervenants

Cornélia FINDEISEN

Directrice générale adjointe chargée de l'Attractivité et de l'Aménagement du Territoire
Communauté Urbaine Le Havre Seine Métropole

D'origine allemande, diplômée d'un DESS en Commerce International et passée par l'ENA, Cornelia Findeisen a exercé dans les secteurs privé et notamment public, où elle a occupé des postes en administrations centrales puis continué sa carrière dans les collectivités territoriales. En tant que directrice générale adjointe de grandes collectivités elle a exercé des missions très variés, portant tant sur le pilotage de projets stratégiques que sur la mise en œuvre opérationnelle des services publics de proximité et du quotidien. Elle s'est fait une spécialité des enjeux de « transformations à l'ère du digital » et des « politiques publiques à l'ère des data ».

Kris DANARADJOU

Directeur Général Adjoint
HAROPA - Port du Havre

Diplômé de l'Ecole Nationale des Travaux Publics de l'Etat et de Sciences Po Grenoble, Kris DANARADJOU a commencé sa carrière au sein du Ministère de l'Equipement et des Transports puis a exercé différentes missions de direction de projets en maitrise d'ouvrage au sein de La Maison de Radio France et du Musée du Louvre. Il rejoint en 2014 HAROPA-Ports de Paris en qualité d'adjoint à la Direction de l'Aménagement puis de Directeur du Port de Gennevilliers, première plate-forme multimodale d'Ile-de-France.
Depuis Juillet 2020, Kris DANARADJOU est Directeur Général adjoint de HAROPA – Port du Havre, premier port pour le commerce extérieur de la France et 5e port nord-européen pour le trafic Conteneurs. Il est plus particulièrement en charge de l'interface avec les collectivités territoriales, du développement de l'innovation digitale et du pilotage de l'ensemble des projets de développement avec un accent tout particulier sur la Multimodalité.

Jean-Marie DUMON

Délégué général adjoint
GICAN

Jean-Marie Dumon est Délégué Général Adjoint, chargé des questions de défense et de sécurité, au GICAN. Diplômé de l'Ecole Navale, de l'ENSTA PARIS TECH, de l'Ecole de Guerre et de l'IHEDN « armement et économie de défense », Jean-Marie DUMON est nommé Délégué à la défense et à la sécurité du GICAN. En tant qu'officier de marine et ingénieur, il a exercé des responsabilités variées pendant plus de trente ans dans la Marine Nationale, dont deux commandements à la mer. Il a également travaillé auprès de nombreuses hautes autorités du Ministère des Armées, en particulier sur la stratégie de réformes.

Expert en essais de navires et en sécurité maritime, ancien président de la grande commission nautique, il a également eu l'opportunité de mesurer les enjeux entrepreneuriaux dans de nombreux secteurs professionnels, en tant que secrétaire général du comité de liaison défense du MEDEF.

Michel CADIC

DPSIS adjoint
Ministère de l'Intérieur

Michel Cadic est ingénieur en chef de l'armement. De spécialité ingénieur armement terrestre (Ensta Br), il bénéficie également d'une formation en économie (Doc) et en droit public (Lic). Il est ancien auditeur du CHEDE.

Ayant commencé sa carrière au ministère de la défense / Délégation Générale pour l'Armement en 1988 par les essais d'engins blindés, dont le char Leclerc, (DGA/Angers), il rejoignit la DGA /DRI en 1997 et fut en charge du soutien à l'exportation pour plusieurs pays du Moyen Orient (DGA/DRI), puis d'activités transverses comme chef de cabinet (2002-2003). Il est ensuite nommé directeur de projet Portail de l'armement, intégrant la place de marchés dématérialisées pour l'ensemble des achats du ministère de la Défense. En 2005, il fût chargé de créer le service de l'attaché d'armement auprès de l'ambassade de France à Stockholm. De retour en France en 2008, il occupa plusieurs postes à caractère financier à la DGA (programme Rafale, démarche d'orientation de la DGA). De 2014 à 2018, il fût en charge d'activités de sécurité économique, de protection d'installations puis de prospective sécuritaire au profit de la sphère défense.
Il a rejoint le Ministère de l'intérieur le 1er septembre 2018, comme Délégué ministériel adjoint aux industries de sécurité et à la lutte contre les cybermenaces.
Il a rejoint le Ministère de l'intérieur le 1er septembre 2018, comme Délégué ministériel adjoint aux industries de sécurité et à la lutte contre les cybermenaces.

Andréas SCHWAB

Député européen
Parlement européen

Dr. Andreas Schwab has been a Member of the European Parliament since 2004. Born in 1973, he studied law at the University of Freiburg and the Institut d'Etudes Politiques in Paris, and obtained an L.L.M. from the University of Wales in 2000. He worked as a consultant for the European Convention in the Department of European Affairs of the Baden-Württemberg State Ministry while obtaining a doctorate in law in 2002 and completing his second state law exam in 2003. He is the EPP Group Coordinator in the Committee on the Internal Market and Consumer Protection, a substitute Member of the Committee on Economic and Monetary Affairs, Chair of the Delegation for Northern cooperation and for relations with Switzerland, Norway, Iceland and the EEA, a member of the Bureau of the EPP Group as well as Chairman of the CDU Südbaden. He has been steering key legislation on competition policy, consumer rights, services and cybersecurity.

Bruno BENDER

Coordonnateur cyber pour le monde maritime
Comité France Maritime

Bruno BENDER est un spécialiste des technologies de l'informations et de communication.
Sa carrière d'officier de marine et sa position actuelle de consultant l'ont amené à évoluer dans le domaine des systèmes de surveillance et de communication maritimes français, européens et OTAN et d'en appréhender leur protection face à la menace Cyber.
Impliqué dans la gouvernance de systèmes nationaux, européens comme EUROSUR et MARSUR ou multinationaux il dispose d'une expertise dans le domaine de l'interopérabilité, et la cybersécurité des systèmes navals.

Jérôme BESANCENOT

Chef du Service du Développement des SI
HAROPA - Port du Havre

Jérôme Besancenot dirige le service des systèmes d'information de HAROPA - Port du Havre. Expert en systèmes d'information portuaires et maritimes, il participe aux développements de guichets électroniques portuaires, systèmes ouverts aux professionnels qui permettent d'améliorer l'organisation des échanges d'information et facilitent le commerce international. L'activité des ports est de plus en plus étroitement dépendante des systèmes d'information qui couvrent un large domaine propre au fonctionnement opérationnel relatif aux flux de marchandises et matières dangereuses ou aux passages des navires dans l'enceinte de la zone portuaire. L'enjeu de la cybersécurité devient une question stratégique pour l'activité du transport maritime.
JérômeBesancenot est membre de comités internationaux sur la dématérialisation des échanges d'information tels le workgroup « Trade facilitation & Port Community System » de l'Association Internationale des Ports (IAPH), le groupe européen PROTECT ou encore le comité « Facilitation of International Maritime Traffic » de l'Organisation Maritime Internationale (OMI).
Jérôme Besancenot est docteur en informatique de l'Université Pierre et Marie Curie (Paris VI) en systèmes d'information distribués et hétérogènes. Il a publié plusieurs articles dans des magazines et revues spécialisés. Il est également co-auteur d'un livre sur les systèmes transactionnels.

Laurent VERDIER

Chargé de mission sensibilisation risque cyber
Cybermalveillance.gouv.fr

Laurent Verdier a rejoint le dispositif Cybermalveillance.gouv.fr en septembre 2020 en tant que chargé de mission pour contribuer à l'animation et au développement de la sensibilisation des publics au risque cyber. Officier de police mis à la disposition du dispositif par le ministère de l'Intérieur, il mettra à profit son expertise en matière de cybercriminalité et son expérience acquises dans ce domaine depuis 2002 à la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) de la Préfecture de Police, à la Direction Centrale du Renseignement Intérieur (DCRI) puis au sein du Centre de Cyberdéfense de l'ANSSI.

Dr Michel DUBOIS

Chef du Pôle Expertise, Direction de la cybersécurité
GROUPE LA POSTE

Michel Dubois est chef du pôle expertise cybersécurité au sein de la direction de la cybersécurité du Groupe La Poste. Ingénieur en informatique, titulaire d'un mastère spécialisé en Sécurité des Systèmes d'information et docteur en cryptologie, Michel a exercé pendant près de trente ans des fonctions de responsable de la SSI au sein du Ministère des Armées. Il est, par ailleurs enseignant chercheur au sein du laboratoire de Cryptologie et de Virologie Opérationnelles de l'ESIEA à Laval. Il est membre du club des experts de la sécurité de l'information et du numérique (CESIN), du club de la sécurité de l'information français (CLUSIF) et de l'association des réservistes du chiffre et de la sécurité de l'information (ARCSI).

Philippe GENOUX

Délégué général
EXERA

Philippe Genoux est depuis juin 2014 le délégué général de l'association Exera regroupant une trentaine de membres, groupes industriels exploitant des équipements de mesure, de régulations et automatismes, ou centres d'essais et d'expertise. Parallèlement, il exerce une activité de consultant indépendant depuis fin 2000, et a mené plusieurs missions de conseil, notamment en ingénierie financière, rapprochement d'entreprises ou stratégie et organisation (voir www.pronoia-consulting.com).
Précédemment, il a occupé de 2009 à 2012 le poste de chef de la mission "Partenariats Public Privés" (PPP) du ministère de la défense, mission qu'il a créée en mars 2009. À la tête d'une équipe d'une douzaine de personnes hautement qualifiées (juristes, analystes et chargés de projets, il a ainsi directement participé à l'ensemble des opérations d'externalisations et des PPP lancés par le ministère de la défense durant cette période. De 2004 à 2009, il occupait le poste de chef du bureau "Nouveaux modes d'acquisition" qu'il a créé en juillet 2004 au sein de la délégation générale pour l'armement (DGA), et, à ce titre, a mené la passation du premier contrat de partenariat du ministère de la défense, notifié en janvier 2008, portant sur la mise à disposition de la base-école de Dax d'une flotte d'une quarantaine d'hélicoptères (durée 22 ans, montant 430 M€ HT).
Philippe Genoux a débuté sa carrière professionnelle au ministère de la défense en 1983 après un stage professionnel d'un an aux États-Unis en tant qu'ingénieur de recherche. D'abord chargé de l'orientation et du financement de projets de recherche, il a ensuite animé de 1985 à 1990 une équipe d'ingénieurs au sein du Bassin d'essais des carènes pour mener à bien la conception de propulseurs innovants destinés aux sous-marins nucléaires lanceurs d'engin types « l'Indomptable » et « le Triomphant ».
Entré en 1991 à Innolion, société de capital risque alors filiale du Crédit Lyonnais, il a constitué et géré un portefeuille de participations, valorisé à 10 M€, dans des sociétés "starts-up" de technologie. Dans le cadre de ses activités, il a été administrateur de sociétés françaises et étrangères (Grande Bretagne, États-Unis, Pays-Bas), et a directement participé à deux introductions en bourse (Londres et Amsterdam) et à de nombreuses cessions industrielles. Parallèlement, de 1994 à 1997, il a été directeur général puis président directeur général de 1994 à 1997 d'une société de robotique médicale détenue par Innolion avant de céder cette société au groupe médical suédois Elekta. À ce titre, il a négocié de nombreux accords (transferts technologiques, accords de distribution, dépôts de brevet).
De 1997 à 2000, il a occupé le poste de Senior Vice-President au sein de la direction centrale des grandes entreprises du Crédit lyonnais. En charge du suivi relationnel de la banque avec ses clients français et étrangers dans les secteurs des équipementiers automobile et des fabricants d'électroménager, il a assuré la coordination des lignes métiers spécialisés de la banque et de son réseau d'agences nationales et étrangères, et, par ailleurs, le dimensionnement des enveloppes financières consolidés en fonction des évaluations de risque global.
Né en 1955, Philippe Genoux est diplômé de l'École Polytechnique (Promotion 1976) et de l'École Nationale Supérieure de Techniques Avancées (1981), et est Docteur de l'Université de Paris VI en Mathématiques Appliquées (1988). Il s'est vu décerné par l'Amicale du Génie Maritime et des Ingénieurs ENSTA le prix Roger Brard en 1993. Il a assuré de 2004 à 2012 de nombreuses formations sur les partenariats public-privé (ENA, IHEDN, CID, CFMD, etc.).
Ingénieur général de l'armement (2S), il est chevalier de la Légion d'Honneur et officier dans l'Ordre national du Mérite.

Les intervenants

Fabien MIQUET

Product & Solution Security Officer
Siemens Digital Industries France

De formation ingénieur généraliste dans les domaines du génie électrique, de l'informatique et des réseaux puis spécialisé dans celui des télécommunications, Fabien Miquet commence sa carrière en 2001 en intégrant *Aérospatiale Matra, fraîchement devenue European Aeronautic Defence and Space Company* (EADS) avant d'être renommé Airbus Group.

Immergé dans le monde passionnant des lanceurs civils et militaires (Ariane 4 et 5, ATV, missile M51, SNLE NG…) et des infrastructures critiques (CIGEO, SECOIA…), il y passera près de 18 années, lui permettant d'endosser de nombreuses responsabilités au sein du groupe Airbus, ayant toutes pour dénominateur commun la Sécurité des Systèmes d'Information (SSI) devenue depuis « Cybersécurité ».

Tour à tour acteur dans les activités d'ingénierie système SSI, les réponses à appel d'offre, les activités de R&D en SSI industrielle, la sensibilisation et la formation en cybersécurité des collaborateurs puis chef de projet sur la problématique de sécurité des infrastructures critiques, il est reconnu en 2016 Expert Product Security du réseau Airbus au sein de la société ArianeGroup.

Cette nomination lui permettra d'une part une participation active dans différents Groupes de Travail dont ceux de l'ANSSI relatifs à la cybersécurité des systèmes industriels ayant conduit à la rédaction des guides du même nom (classification des installations, description des mesures détaillées). Elle lui permettra d'autre part le maintien, la capitalisation et la dissémination de ses connaissances en parallèle d'activités techniques diverses et variées, en agissant de manière transverse sur les grands programmes du groupe.

En 2018, Fabien rejoint avec la même ferveur le groupe Siemens, d'abord en tant que Product & Solution Security Expert (PSSE) au sein de la division « Building Technologies » devenue depuis avril dernier « Smart Infrastructures ». Il est nommé en 2019 Product & Solution Security Officer (PSSO) de la division Digital Industries du groupe Siemens pour la France et a pour missions, entre autres, de continuer à faire de Siemens un partenaire de confiance, leader en matière de cybersécurité des systèmes industriels automatisés et de porter les certifications et qualifications ANSSI des produits de la division, parmi lesquels la gamme S7-1500, seuls automates à ce jour qualifiés par les autorités françaises.

Dr Florence LECROQ

Maître de Conférences
Université du Havre Normandie

Dr Florence LECROQ, Maître de Conférences à l'Université Le Havre Normandie, enseigne l'automatisme et la cybersécurité des systèmes industriels dans deux formations labellisées CyberEdu : le DUT GEII - Génie Électrique et Informatique Industrielle et License Professionnelle SARII SII - Systèmes Automatisés, Réseaux et Informatique Industrielle Supervision des Installations Industrielles) de l'IUT du Havre.

Colonel Florian MANET

Commandant la Section de Recherches Bretagne
Gendarmerie Nationale

Diplômé de l'école spéciale militaire de saint Cyr (1998) et de l'école de guerre (2011).
Après un début de carrière militaire au sein de l'armée de terre, Florian Manet rejoint la gendarmerie nationale, en 2004, où il commande successivement des unités de maintien de l'ordre et de sécurité publique.
Entre 2011 et 2015, Florian Manet exerce les responsabilités de conseiller sûreté du secrétaire général de la SNCF. Au sein de la direction de la sûreté, il dynamise un partenariat opérationnel et stratégique entre la compagnie ferroviaire et la gendarmerie, en particulier, en matière de gestion de crise liée à un événement ferroviaire ainsi qu'en matière de protection des infrastructures et de continuité du service public de transport de voyageurs. Son action s'est inscrite naturellement dans le cadre d'un meilleur partenariat. Ainsi, fortement impliqué dans la problématique des atteintes au réseau national, il a fondé et animé des groupes de travail inter-entreprises au sein du CDSE (Club des Directeurs de Sûreté d'Entreprises) comme au sein d'instances européennes dédiées.
Avant d'être nommé commandant de la section de recherches Bretagne, Florian MANET a dirigé la section de recherches de la gendarmerie maritime, le service national de police judiciaire de la mer. En coordination étroite avec les acteurs privés comme publics, il a développé une approche renouvelée de la lutte contre la criminalité organisée (cybercrime, atteinte au patrimoine naturel maritime, trafic d'êtres humains, terrorisme..) en lien avec l'environnement maritime et les gens de mer. De plus, dans le cadre du cycle politique de 2018-2021 de l'Union européenne, cet officier est leader d'un projet européen EMPACT (European Multiapproach Platform Against Criminal Threat)-EUROPOL dédié à la criminalité organisée spécialisée sur les atteintes au patrimoine naturel maritime.
Il a écrit divers articles consacrés aux cyber-menaces comme à la lutte contre la criminalité organisée. Il est l'auteur d'un ouvrage intitulé « *Le crime en bleu, essai de thalassopolitique* », publié aux éditions Nuvis en mai 2018.

Gildas REUL

Responsable du Pôle Sûreté et Continuité d'Activité
HAROPA - Port du Havre

YDiplômé d'un DESS en droit et stratégie de la sécurité intérieure puis de l'école des officiers de la Gendarmerie Nationale, Gildas REUL, 55 ans, a débuté sa carrière au sein de la Marine Nationale pendant 6 ans. Il rejoint ensuite la Gendarmerie Nationale où il y occupe divers postes de commandement d'unités opérationnelles et d'état-major auprès des ministères, préfectures judiciaires et services d'enquêtes.
Il rejoint HAROPA-Port du Havre en 2018 en qualité de Responsable du Pôle Sûreté et continuité d'activité.

Yann VACHIAS

Directeur général adjoint
Ecole Nationale Supérieure Maritime

Yann VACHIAS est le directeur général adjoint de l'Ecole Nationale Supérieure Maritime (ENSM). Après une première carrière de navigant, il a rejoint l'école nationale de la marine marchande de Marseille comme enseignant en sciences nautiques avant d'exercer successivement les fonctions de chef de département sciences nautiques, directeur du site de Nantes de l'ENSM, directeur du développement et des partenariats et directeur de la recherche (fonction qu'il exerce toujours) du même établissement

Dans le cadre de cette dernière mission, il a piloté le développement de la cybersécurité au sein de l'école et notamment la mise en place de la plateforme cybersécurité, le développement de cours au profit des étudiants et la participation de l'école au projet SMART PORT CITY.

Cyril CHEDOT

Responsable du Service Planification de l'Aménagement du territoire
HAROPA - Port du Havre

Cyril Chédot, Docteur en Géographie, est en Charge du Service Planification de l'Aménagement du territoire au Grand Port Maritime du Havre. Il est impliqué dans l'animation de l'écosystème d'innovation autour des ports de HAROPA, au travers de partenariats avec divers laboratoires (UMR IDEES – DEVPORT), le montage de projets collaboratifs (Smart Car Terminal) et la tenue d'événements d'animation comme les Hackathons Smart Port de HAROPA depuis 2016. Impliqué dans le projet Le Havre Smart Port City, lauréat du PIA3 en 2019, il est en charge de la coordination des projets portuaires et plus particulièrement du 5G Lab, qui réunit Nokia, Siemens, EDF, la communauté urbaine Le Havre Seine Métropole et le GPMH.

Cyrille BERTELLE

Professeur
Université Le Havre Normandie

Cyrille Bertelle est professeur des universités à l'université Le Havre Normandie depuis 2005. Ses activités de recherche portent sur la modélisation et la simulation des systèmes et réseaux complexes appliqués aux systèmes territoriaux et logistiques afin de produire des outils d'analyse et de reconstruction numérique de la complexité des territoires pour l'ingénierie de l'intelligence territoriale dans les smart cities et les smart ports. Plus récemment, il travaille sur l'intégration de blockchains dans les transactions logistiques, en réponse à un grand nombre d'attentes des opérationnels du territoire qui se tournent vers les futures générations des systèmes d'informations pour la logistique. Il est auteur de plus de 45 publications en revues scientifiques internationales et plus de 100 communications en conférences internationales. Il est coordinateur de 3 livres chez Springer Verlag. Il a été invité comme keynote speaker dans une dizaine de conférences internationales (Paris, Portugal, China, Roumania, Jordan, Algeria, Tunisia, Korea, Spain, UK). Il a dirigé 18 thèses de doctorats.

William LECAT

Directeur de programme Grand Défi automatisation de la cybersécurité
Secrétariat Général pour l'Investissement

Avant d'être Directeur de programme Grand Défi automatisation de la cybersécurité pour le Secrétariat Général pour l'Investissement, William LECAT était précédemment chef d'un département de trente ingénieurs spécialisé dans le développement logiciel d'outils de cyberdéfense au sein de la Délégation générale pour l'armement (DGA).

Auparavant, il a occupé le poste d'adjoint au responsable du pôle SSI de la DGA, en charge des études amont, des relations avec l'ANSSI et avec les industriels.

Il est diplômé de l'Ecole Polytechnique et titulaire d'un Master of Science de GeorgiaTech en sécurité de l'information.

Christophe AUBERGER

Directeur Technique - Evangéliste Cybersécurité
Fortinet

Titulaire d'un master en Informatique et Telecom et après quelques années au service des contre-mesures au sein de la marine nationale (DPSD), il oriente sa carrière vers l'IT et prend la responsabilité du support chez Altis Informatique.

Il gère ensuite l'avant-vente et le consulting de l'entité de gouvernance des systèmes d'information chez ARCHE Communications.

Dans les années 2000, il est co-fondateur et directeur technique du premier MSSP français : monDSI.com qui prendra des parts de marché significatives dans le domaine avant d'être intégré au groupe RISC.

Ensuite Christophe rejoint Fortinet et prend la direction de l'avant-vente.

Actuellement, il est responsable technique France, et intervient en tant qu'expert auprès des grands clients et des institutions.

Olivier LASMOLES

Professeur associé en droit portuaire, chef du département supply chain management et sciences de la décision
EM Normandie

Titulaire d'un doctorat en droit privé de l'Université Paris I Panthéon-Sorbonne, Olivier LASMOLES est professeur associé de droit à l'Ecole de Management de Normandie. Il est Directeur du Département Supply-Chain Management & Sciences de la décision. Il intervient dans les domaines du droit maritime, du droit de l'environnement et du cyber-droit. Il enseigne, depuis plus de 10 ans, le droit maritime et le droit de la sécurité maritime en Master 2 « Droit de la mer et risque maritime » à l'Université Lille 2. Par ailleurs, il est membre du comité de rédaction de la revue Préventique et membre du Comité Directeur de l'Association Française du Droit Maritime. Enfin, il est officier de réserve opérationnel de la Marine Nationale spécialité Etat-major depuis 10 ans. Il est actuellement Adjoint Protection-Défense du Commandant de la Marine du Havre. Il est également auditeur IHEDN et membre du Comité Exécutif de l'AR11.

Les intervenants

Yvon KERMARREC

Titulaire
Chaire de cybersécurité des systèmes navals

Yvon Kermarrec est Professeur en informatique à IMT Atlantique et fut membre du comité de direction de IMT Atlantique en tant que responsable de département. Il a obtenu le doctorat en informatique puis l'habilitation à diriger les recherches.
Ses activités de recherche et d'enseignement sont en lien avec les systèmes distribués, la sécurité, le génie logiciel et la fiabilité logicielle. Il a été chercheur au Courant Institute de New York University (NYU), architecte logiciel avec Raytheon (Vancouver, BC) avant de rejoindre Telecom ParisTech puis Télécom Bretagne en tant qu'enseignant-chercheur.
Depuis 2016, Yvon Kermarrec est titulaire de la chaire de cybersécurité des systèmes navals, qui implique Naval Group, Thales, la Marine nationale, l'Ecole navale, l'ENSTA Bretagne et IMT Atlantique. Il encadre et dirige l'équipe de recherche de la chaire et coordonne les activités scientifiques en lien avec les partenaires industriels et la Marine.
Yvon Kermarrec est responsable pédagogique du nouveau mastère spécialisé consacré à la cybersécurité des systèmes maritimes et portuaires, en lien avec l'Ecole navale, l'ENSTA Bretagne, l'ENSM et IMT Atlantique.

Pedro MERINO LASO

Chargé de recherche
Ecole Nationale Supérieure Maritime

Pedro MERINO LASO est chargé de recherche à l'École Nationale Supérieure Maritime (ENSM). Il fait des recherches dans le domaine de la cybersécurité maritime dans cette école depuis 2018 traitant des sujets divers : navires autonomes, analyses de risques, détection d'attaques, formation des marins...
Auparavant, il a réalisé son doctorat dans la Chaire de cyberdéfense des systèmes navals basée à l'École Navale en partenariat avec l'IMT Atlantique, Thales et Naval Group. Ses travaux de thèse ont traité la détection de dysfonctionnements et d'actes malveillants dans des flux de données capteur.
Actuellement, il est enseignant et un des responsables pédagogiques du nouveau Mastère spécialisé® Cybersécurité des systèmes maritimes et portuaires. Cette formation est unique en Europe et elle a été créée par quatre écoles d'ingénieurs : l'IMT Atlantique, l'ENSTA Bretagne, l'École Navale et l'ENSM. Aussi, il réalise des cours de sensibilisation à profit des élèves de l'ENSM.

Carl HERNANDEZ

Co-fondateur
Avant de cliquer.com

Après une carrière dans la grande distribution en tant que directeur de secteur puis démarqueur financier dans des enseignes telles que IKEA ou Carrefour groupe, Carl Hernandez s'est passionné pour la formation.

Formateur certifié d'état, Carl HERNANDEZ a ensuite cofondé la société « Avant de Cliquer », qui propose une solution de cybersécurité permettant une montée en compétences des utilisateurs face aux attaques par phishing.

Stéphane FRONCZAK

Chef de la cellule CYDERGENDMAR
Gendarmerie Maritime

C'est en 1994 que ce passionné de la mer intègre la gendarmerie maritime pour y connaître sa première affectation à Brest. Après 10 ans et trois unités différentes, il quitte la cité du Ponant pour œuvrer deux ans à Nouméa. De retour en métropole, de 2006 à 2009, il exercera les fonctions de chef de service d'un service administratif au sein du commandement de la gendarmerie maritime. Mais l'envie d'exercer la police judiciaire est toujours présente et c'est en 2009, à l'occasion de la création de la brigade de recherches du Havre qu'il rejoint la Normandie, en qualité de commandant adjoint. En 2010, il devient le premier enquêteur en nouvelles technologies (Ntech) de la gendarmerie maritime ; il découvrira toute l'étendue de la cybercriminalité au sein des infrastructures maritimes et portuaires jusqu'en 2014, ou il rejoint Toulon pour devenir responsable des investigations numériques au sein de la Section de Recherches de la gendarmerie maritime. Depuis, tout en exerçant ses compétences judiciaires, il poursuit la formation de nouveaux enquêteurs Ntech (tutorat) tout en se formant sur les appareils électroniques embarqués (AIS, VDR, ECDIS, SCADA) ; il procède à la réalisation d'un réseau de correspondants numériques au sein de la gendarmerie maritime sur tout le territoire national (42 personnels), effectue des interventions de préventions, sensibilisation auprès des acteurs maritimes civils et militaires ainsi que des ateliers (Rencontre Parlementaire Cyber Cercle – Cluster Maritime Français – Armateurs de France) et participe à différents exercices de lutte cyber (Britanny Ferries – Orange maritime – lutte contre le contreterrorisme maritime). Chef de la cellule Cybergendmar depuis 2018 et disposant d'une expertise en cybercriminalité maritime, il réalise en 2019 avec le commandant de la SR de la gendarmerie maritime un voyage d'études cybercriminalité maritime auprès des US Coast Guards (WashingtonCharleston-Miami). Dernièrement, après avoir dirigé l'enquête de l'incendie du SNA PERLE, c'est en septembre 2020, qu'il participe en compagnie d'autres unités de la gendarmerie nationale (Section de Recherches de Marseille – C3N de Pontoise – GIGN), à la première enquête judiciaire cybercriminelle coordonnée lors de l'attaque par ransomware de l'armement français CMA CGM.

Julien PREVEL

Membre du Directoire, en charge de la transformation digitale entreprise, Directeur des Ressources Humaines
SOGET

Julien PRÉVEL est Directeur des Ressources Humaines et Membre du Directoire, notamment en charge de la transformation digitale de SOGET.
Diplômé d'un Bachelor of Arts (B.A.) de Business Management de l'Université d'Edimbourg et d'un DESS en Commerce international, Vente et Marketing de l'Université Le Havre Normandie, Julien PRÉVEL commence sa carrière chez BOLLORE Logistics en 2003 et intègre SOGET en 2005 pour y exercer des responsabilités commerciales puis de chef de produit. Il a notamment piloté la mise en place des échanges Import Control System (ICS) de sûreté/sécurité en faisant de SOGET un partenaire EDI certifié et tiers de confiance pour les échanges informatiques avec l'ensemble des Douanes de l'UE.
En 2012, il se voit confier la responsabilité du service Méthodes, Qualité et Systèmes d'information, dirigera la mise en œuvre des procédures organisationnelles de l'entreprise et des systèmes d'information pour le maintien et l'évolution de la Qualité. Parallèlement, il endosse le rôle de Responsable Support Clients et dirige le chantier d'industrialisation de la Gestion des Incidents et de la relation clients via la mise en œuvre d'un CRM.
Son expertise acquise au sein de SOGET lui confère une connaissance approfondie des différents métiers exercés chez SOGET ainsi qu'une connaissance des clients, partenaires et de l'environnement de l'entreprise. C'est ainsi qu'il est nommé Directeur des Ressources Humaines en 2016 et intègre le Directoire de SOGET en 2018.

Alexandra BIGAS

Membre
CEFCYS

Experte certifiée CISSP ayant débuté il y a 20 ans dans l'administration de systèmes, réseaux et sécurité, puis ayant progressivement évolué vers des métiers de conseil et gouvernance cybersécurité et devenue consultante freelance en 2019.
Elle est membre du CEFCYS, le Cercle des Femmes de la Cybersécurité.

Laurane RAIMONDO

Chercheure associée
Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense

En 2014 d'abord, puis en 2016, pendant ses études, Laurane RAIMONDO travaille pour la data unit du Conseil de l'Europe. En 2018, ses travaux mêlent la protection des données, le cyber et la question de la militarisation et l'arsenalisation de l'espace extra-atmosphérique. Ses recherches sur ce dernier sujet sont primées par le prix du Gouverneur militaire de Lyon. Exerçant dans le même temps comme data protection officer auprès d'un organisme traitant des données sensibles de personnes vulnérables, elle développe l'enseignement cyber dans le Master Relations Internationales à la Faculté de Droit à l'Université Jean Moulin Lyon 3 et celui des données personnelles dans le parcours Expertise et Risques Internationaux. Auteure de l'ouvrage La protection des données personnelles en 100 questions-réponses à paraître chez Ellipses début 2021, elle écrit pour la série Stories of Conflict d'Arte, le magazine Sécurité & Défense et entend poursuivre l'écriture à destination du grand public ainsi que l'enseignement. Deux axes visant à rendre le cyber accessible à tous pour développer la confiance dans l'espace numérique.

Jean-Michel VILLEVAL

Délégué général
SYNERZIP-LH

Lieutenant-colonel de sapeurs-pompiers au sein du SDIS 76 jusqu'en novembre 2020
Chef de corps des sapeurs-pompiers de la ville du HAVRE de 1993 à 2000
Chef de l'arrondissement du Havre de 2000 à 2012
Chef de groupement de la formation départementale de 2012 à 2014
Mis à disposition de la plateforme industrielle de la zone industrielle et portuaire du HAVRE site de TOTAL plateforme de Normandie de de 2014 à 2016
Délégué général de l'association SYNERZIP-LH qui réunit les sites industriels et les entreprises de la zone industrielle du HAVRE.

RENCONTRES CYBERSÉCURITÉ NORMANDIE

MERCI À NOS PARTENAIRES & SOUTIENS

HAROPA - Port du Havre, 1er port français pour le commerce extérieur

Bénéficiant d'une situation exceptionnelle sur la façade maritime ouest de l'Europe, HAROPA - Port du Havre, 1er port français pour le commerce extérieur et 5e port nord-européen pour le trafic conteneurs, accueille chaque année près de 6 000 navires parmi lesquels les plus grands porte-conteneurs du monde. Accessible 24h/7j, il traite plus de 70 millions de tonnes de marchandises chaque année et assure près de 40% des importations françaises de pétrole brut.

Membre de HAROPA, 1er système portuaire français, aux côtés des ports de Rouen et Paris, Le Havre constitue une ouverture maritime rapide sur les continents pour tous les armements mondiaux avec près de 600 ports touchés.

Comptant parmi les plus grands ensembles portuaires européens, HAROPA dispose de près de 500 hectares de foncier disponible ou aménageable le long de l'axe Seine. Il accompagne ses clients dans la mise en place et la gestion de systèmes logistiques compétitifs et durables pour desservir le 1er bassin de consommation européen fort de 25 millions d'habitants.

www.haropaports.com

HAROPA

Alliance des ports du Havre, de Rouen et de Paris

- 5e ensemble portuaire nord-européen ;
- 1er port à conteneurs français pour le commerce extérieur ;
- 1er port intérieur français et 2e européen ;
- 1er port exportateur de céréales pour l'Europe de l'Ouest ;
- 1er port intérieur mondial pour le tourisme ;
- réélu « Best Seaport in Europe » en 2019.

HAROPA - Port du Havre

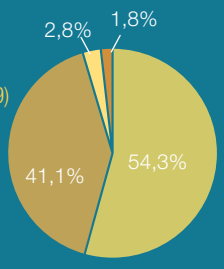
- port fondé en 1517 à la demande de François 1er ;
- accessible 24h/24 et 7j/7 sans contrainte de marées pour les porte-conteneurs de plus de 20 000 EVP à pleine charge ;
- 1er port d'Europe du Nord touché à l'import et dernier port d'escale à l'export ;
- 1er port mondial pour le transport des vins et spiritueux ;
- 1re plateforme française pour l'import-export de véhicules neufs.

Chiffres clés

- Circonscription portuaire
  - superficie de 27 km, pour 5 km de large, de l'entrée du port jusqu'aux écluses de Tancarville (plus que Paris intra-muros) ;
  - 50 % du territoire portuaire placé en zone naturelle protégée ;
  - 150 km de routes, 200 km de voies ferrées et 35 km de quais ;
  - 100 manœuvres de ponts et écluses par jour ;
  - près de 1150 établissements implantés sur la zone industrialo-portuaire (ZIP) ;
  - près d'1 million de m² d'entrepôts logistiques ;
  - plus de 30 000 emplois générés par l'activité de la zone portuaire.
- Trafics
  - près de 700 ports touchés dans le monde avec la présence de 50 armements au Havre ;
  - plus de 60 allers-retours ferroviaires par semaine ;
  - 5 000 escales en moyenne par an ;
  - près de 70 Mt de trafic maritime et fluvial en 2019
    - ↳ dont près de 3 millions d'EVP (équivalent vingt pieds) ;
  - près de 354 400 passagers croisière accueillis en 2019.

Répartition du trafic maritime (2019)

- Vracs liquides (36,13 Mt)
- Conteneurs (27,3 Mt)
- Vracs solides (1,22 Mt)
- Autres (1,84 Mt)



Certifications

- qualité : ISO 9001 pour l'accueil des navires, l'accueil et la vie sur le domaine portuaire et la gestion des réseaux de dessertes ferroviaires et routières ;
- sûreté : ISO 28000 (1er port européen et 2e mondial à détenir cette certification) ;
- environnement : PERS (Port environmental review system).

LE HAVRE port
HAROPA

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

PARTICULIERS, ENTREPRISES, COLLECTIVITÉS TERRITORIALES :

VOUS ÊTES **VICTIME D'ACTES MALVEILLANTS** SUR INTERNET ?

PIRATAGE

ARNAQUE

CHANTAGE

VIRUS

RENDEZ-VOUS SUR
WWW.CYBERMALVEILLANCE.GOUV.FR
POUR ÊTRE ASSISTÉ
ET CONSEILLÉ

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

MISSIONS
DU DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

1. **ASSISTANCE AUX VICTIMES** D'ACTES DE CYBERMALVEILLANCE
2. **INFORMATION ET SENSIBILISATION** SUR LA SÉCURITÉ NUMÉRIQUE
3. **OBSERVATION ET ANTICIPATION** DU RISQUE NUMÉRIQUE

MEMBRES

PREMIER MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

SECRÉTAIRE D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES

AFCDP · afnic · ATEMPO · WOOXO GROUP · BANQUE des TERRITOIRES · Bitdefender · bouygues · CCR · CCR RE · CHAMBRE DE COMMERCE ET D'INDUSTRIE · CDSE · CESIN · CINOV NUMÉRIQUE · CLCV · CLUSIF · CNLL · coTer numérique · Cevea · cpme · CROWDSTRIKE · DÉCLIC · EBEN · e-Enfance · eset · Fédération Française de l'Assurance · fevad · FRANCE VICTIMES · Google · hp · Hub One Digital Technologies · INC · kaspersky · LE GROUPE LA POSTE · MAIF · MEDEF · Microsoft · Neuflize OBC · Orange Cyberdefense · SFR BUSINESS · signal spam · STORMSHIELD · syntec numérique · UFC QUE CHOISIR

PLUS D'INFORMATIONS SUR **WWW.CYBERMALVEILLANCE.GOUV.FR**

FORTINET®

CONÇU POUR SÉCURISER VOS OPÉRATIONS GRÂCE À L'INTELLIGENCE ARTIFICIELLE

Protège, détecte et répond aux cyberattaques à la vitesse de l'IA

www.fortinet.fr

L'INTELLIGENCE ARTIFICIELLE, MOTEUR POUR AVANCER DANS UN MONDE COMPLEXE

Depuis début 2020, le monde entier vit l'une des « reprogrammations » les plus importantes de l'histoire du numérique. Les réseaux ont été profondément impactés par ces millions d'utilisateurs qui ont soudainement migré, parfois en l'espace d'une nuit, vers la périphérie (edge) du réseau corporate, pour continuer à assurer leurs missions en télétravail. Avec ce bouleversement qui impacte nos plans de continuité métier et de reprise d'activité, de nombreux organismes ou entreprises se sont rendus brusquement compte que leurs pare-feux traditionnels n'offraient pas l'évolutivité nécessaire pour accompagner l'expansion massive de leur périphérie de réseau (edge network). Ils ont dû, dans l'urgence, mettre à jour leurs dispositifs, voire déployer de nouvelles appliances pour répondre à la demande de leurs télétravailleurs.

En parallèle, l'environnement technologique des entreprises, et de notre société en général, gagne en complexité. Les villes intelligentes comptent désormais sur des leviers comme l'IA pour piloter leurs services urbains : trafic routier, électricité ou encore les systèmes d'urgence. Les environnements multisites de production industrielle en tirent également parti pour répondre à la demande des consommateurs en quasi-temps réel. Les data centers d'envergure dépendent de systèmes intelligents pour traiter les méga-flux d'informations (elephant flows) utilisés pour les traitements informatiques et les modélisations complexes. Les plateformes de trading financier misent sur l'IA pour effectuer des transactions à la microseconde près, suivant l'analyse de flux massifs de données.

Mais ceci n'est qu'un début. Pour tenir la cadence, l'IA devra aller plus loin, plus vite. La 5G, associée à des périphériques toujours plus intelligents et à des services multimédias riches, sera bientôt en mesure de créer des réseaux edge dynamiques qui changeront fondamentalement la façon dont les données sont générées, distribuées et utilisées. Ajoutez à cela des milliards d'objets connectés semi-intelligents et des ressources dynamiques de routage positionnées sur l'edge, augurant un changement radical qui affectera notre façon de travailler et de vivre.

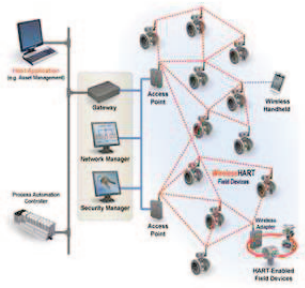
Cette transition vers de nouveaux environnements plus complexes exige d'optimiser les performances et l'évolutivité, ce qui signifie que les décisions critiques doivent être prises instantanément, de façon transparente et de manière cohérente. En matière de sécurité, il en résulte que les entreprises se tournent vers l'apprentissage automatique et l'IA pour gérer leurs réseaux dynamiques et complexes. Les systèmes de sécurité optimisés par l'IA, associés à des technologies fiables et temps réel de veille sur les menaces, concrétisent une approche réseau orientée sécurité opérant en tant que système unifié.

Dans ce contexte nouveau, l'innovation est essentielle pour nos clients et est présente avant toute chose dans la Fortinet Security Fabric, **un écosystème étroitement intégré et packagé qui offre une réelle différenciation en matière de sécurité.** Cette plateforme apporte une gouvernance et une gestion simplifiées, une plus grande efficacité opérationnelle, la préservation des ressources rares, difficiles à acquérir et à retenir grâce à l'automatisation et une amélioration significative du niveau de sécurité par la synergie inter-fonctions

Fortinet se classe au premier rang des appliances de sécurité commercialisées dans le monde et plus de 480 000 clients nous font confiance pour protéger leurs entreprises. À la fois entreprise de technologie et de formation, le Fortinet Network Security Expert (NSE) propose aujourd'hui l'un des programmes de formation en cybersécurité les plus importants et les plus vastes de l'industrie.

Pour en savoir davantage :
https://www.fortinet.com/fr, le blog Fortinet ou FortiGuard Labs.

Association des EXploitants d'Équipements de mesure, de Régulation et d'Automatismes



- **Une trentaine de membres, de la PME à la multinationale**
- **Une douzaine de commissions techniques (+ de 60 réunions par an, 80 experts actifs au sein des commissions)**
- **4 à 5 évaluations d'équipements lancées dans des laboratoires chaque année à la demande des membres**
- **Bibliothèque en ligne de rapports d'évaluation et de guides de bonnes pratiques (+ de 200 documents)**
- **1 Hot-Line pour les échanges d'informations techniques rapides entre nos membres**
- **1 à 2 journées techniques par an, ouvertes aux non-membres**

Exera |4 Cité d'Hauteville | 75010 Paris | France
Tél : +33 1 53 32 80 08 | Mail : contact@exera.com
Site : www.exera.com

SIEMENS
Ingenuity for life*

Société : Siemens SAS
Adresse : 40, avenue des Fruitiers - 93210 Saint-Denis (France)
Tel : +33 1 85 57 00 00
Site Web :
https://new.siemens.com/fr/fr/entreprise/thematiques/la-cybersecurite-chez-siemens.html

Spécialisations :

Grâce à son approche holistique, Siemens est le partenaire de référence et de confiance pour répondre aux enjeux de la digitalisation et de la cybersécurité des systèmes industriels. En effet, Siemens est le premier équipementier – et le seul à ce jour – à avoir obtenu en France la qualification de l'ANSSI pour une gamme complète d'automate programmable (Simatic S7-1500) et la certification d'un commutateur industriel (Scalance XM400).
Par ailleurs, Siemens accompagne la sécurisation des installations au travers d'un large portfolio de services : cartographie, conseil (IEC 62443, analyse de risques, référentiels ANSSI…), durcissement des configurations, cloisonnement des réseaux, automates industriels sécurisés, switch industriels sécurisés, accompagnement à l'homologation et maintien en condition de sécurité.

Contact :
Fabien Miquet
PSSO Siemens Digital Industries France
fabien.miquet@siemens.com

Depuis plus de 170 ans en France, le nom de Siemens est synonyme de performance technique, d'innovation, de qualité et de fiabilité. Siemens opère dans les domaines de l'électrification, de l'automatisation et de la digitalisation et compte parmi les principaux fournisseurs de technologies à haute efficacité énergétique, qui contribuent à préserver les ressources naturelles. L'entreprise est pionnière en matière d'équipements d'automatisme, de systèmes d'entraînement et de solutions logicielles destinées à l'industrie. Avec plus de 7 000 collaborateurs, 8 sites industriels et 11 centres de R&D dont 8 à responsabilité mondiale, Siemens France s'engage activement dans les filières stratégiques pour l'industrie française. Depuis 2017, Siemens est le seul équipementier dont les process de développement sont certifiés sur la base de la Norme internationale IEC 62443-4-1 par le TÜV Sud, et également le seul à offrir des automates programmables industriels qualifiés par l'ANSSI.
Excellence par ailleurs renouvelée :

- avec le maintien en qualification obtenue en 2019 pour la gamme des automates S7-1500
- avec la labellisation SecNumEdu de sa formation Cybersécurité des systèmes industriels (SITRAIN DI-CYBER)
- avec notre SCADA WinCC Open Architecture (WinCC OA) doublement certifié, autant côté process de développement que côté produit

L'ensemble de ces distinctions montre combien le sujet cybersécurité est un enjeu stratégique pour le groupe. Associant la parole aux actes, Siemens est l'initiateur de la « Charter of Trust » pour promouvoir le sujet cybersécurité au plus haut niveau au sein des entreprises.

Suivez-nous sur Twitter
@Siemens_France

Offre

Gamme complète d'automates industriels sécurisés, switch industriels sécurisés, surveillance de la sécurité des systèmes industriels

Gamme complète d'automates industriels S7 1500 qualifiée

Certifications

Switch industriels SCALANCE XM400, certifiés

Services

Un ensemble de services pour un accompagnement personnalisé :

- Diagnostic (cartographie, analyse de risques, évaluation de la maturité…)
- Conseil (gouvernance, formation…)
- Déploiement (cloisonnement réseau, durcissement des configurations…)
- Contrôle, validation, conformité (préparation à l'homologation, audit de conformité…)
- Maintien en condition de sécurité (mise à jour, gestion des vulnérabilités…)

« La certification TÜV SÜD IEC62443-4-1 de nos sites de développement associée à la certification ANSSI permet à Siemens d'atteindre le niveau le plus exigeant préconisé par l'ICCF Framework issu du groupe de travail de la commission européenne JRC dans le cadre de ses propositions pour une certification européenne des produits pour les systèmes industriels. Nous nous félicitons de cette nouvelle avancée ».

Vincent Jauneau, directeur Digital Industries chez Siemens France. Ⓟ photo Vincent Jauneau

* L'ingéniosité au service de la vie

CYBER

UNE STRATÉGIE AU SERVICE DES ADHÉRENTS DU GICAN

LE GICAN

FÉDÉRATEUR DE L'INDUSTRIE NAVALE FRANCAISE

Le **Groupement des Industries de Construction et Activités Navales** fédèrent aujourd'hui près de 200 industriels, qui participent à la conception, la construction, la maintenance et la réparation des navires civils et militaires.

Enjeu connu de longue date par les industriels aux activités militaires, la cybersécurité prend une ampleur nouvelle pour les activités civiles, et pour l'ensemble des clients et utilisateurs des entreprises de l'industrie navale française. Afin de protéger des navires plus connectés, plus numériques et plus autonomes, les industriels navals français se mobilisent pour fournir à leurs clients les technologies de pointe afin de se prémunir contre des attaques toujours plus élaborées.

Aux côtés de ses adhérents, le GICAN mène une action volontariste sur les problématiques de cybersécurité, afin de participer à l'émergence d'une véritable filière de cybersécurité maritime et de faire valoir les solutions des entreprises françaises.

MISE EN PLACE DE STRUCTURES DÉDIÉES A LA CYBERSECURITÉ MARITIME

Le GICAN mène action une action structurante dans la mise en place du Conseil Cyber du Monde Maritime (C2M2), et participe activement à des Comités de travail autour de l'analyse des risques, de la prospective et de la régulation. Le GICAN anime les actions du collège des industriels, et soutient et met en valeur les positions des adhérents du GICAN, productrices ou consommatrices de solutions cyber pour le naval.

Le GICAN a apporté son soutien et son expertise aux acteurs engagés autour de l'établissement d'un futur centre d'analyse et de réponses aux cyberattaques maritimes (CERT-M).

INFLUENCE ET CRÉATION D'UN ÉCOSYSTEME

Le GICAN intervient dans de nombreux cercles de réflexion sur le sujet de la cybersécurité maritime, notamment au sein des Jeudis de la Sécurité (MILIPOL), dans les travaux du Cybercercle, au MEDEF International ou lors de conférences et entretiens internationaux.

SUIVEZ NOTRE ACTUALITÉ

@GICAN_InduNav

@GICAN

www.gican.fr

FORMATIONS

Le GICAN appuie enfin les travaux relatifs à la formation, la certification des équipements embarqués et la mise en place d'une plateforme portuaire sécurisée.

RÉSEAU

Le GICAN vous accompagne dans la mise en relation et la connaissance de vos produits auprès des leaders d'opinion, prescripteurs et clients.

VOTRE CORRESPONDANT

Jean-Marie DUMON
Délégué Général Adjoint
jean-marie.dumon@gican.asso.fr
+33 (0)6 84 12 91 95

CERCLE DES FEMMES DE LA CYBERSÉCURITÉ

200 femmes impliquées dans les métiers et les enjeux de la cybersécurité

Paris • Toulouse • Rennes • Lille • Marseille • Lyon

www.cefcys.com contact@cefcys.com www.linkedin.com/company/cefcys

@CEFCYS_Officiel facebook.com CEFCYS

LE CEFCYS EN ACTION

Les actions du CEFCYS visent à animer une communauté de femmes travaillant ou aspirant à contribuer au domaine de la Cybersécurité:

- Valoriser et professionnaliser les compétences des femmes via des groupes de travail, des programmes de mentorat, des publications de newsletters et de rapports…

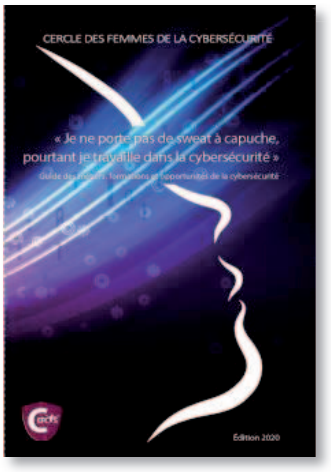
- Organiser et/ou participer à des évènements, des conférences en France et à l'international.

- Sensibiliser les entreprises, les partenaires éducatifs, les recruteurs à l'importance de la parité homme/femme et faire ainsi progresser la présence et l'impact des femmes.

- En action citoyenne, le CEFCYS contribue à sensibiliser le grand public à la cybersécurité, en particulier les jeunes, pour la protection et l'éducation à l'usage sécurisé du numérique.

4 mots clés

Sensibiliser
Éduquer
Prévenir
Protéger



Parmi nos actions 2019…

- Publication du livre « Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité » : un guide inédit à destination des lycéens, parents, éducateurs, femmes souhaitant faire évoluer leur projet professionnel…
- Partenariat avec la Wild Code School pour la formation « analyste cybersécurité »: le CEFCYS a collaboré à la définition du contenu de la formation. La première promotion de 15 élèves est 100% féminine..
- Fondation européenne Women4Cyber : CEFCYS aspire à représenter la fondation européenne Women4Cyber en France, et militera dans ce sens derrière sa présidente.

LES JEUNES IHEDN

ENGAGEMENT

De la jeunesse

Les Jeunes IHEDN est la **première association européenne** et générationnelle sur les questions d'engagement, de défense et de sécurité. Elle est **sous le double parrainage de la ministre des Armées** et du **chef d'état major des armées**.

L'association regroupe les **auditeurs jeunes** formés par l'Institut des hautes études de défense nationale et s'ouvre à **l'ensemble de la jeunesse**.

Plateforme d'**engagement** et **réservoir de réflexions**, l'association offre, en France et à l'international, différents moyens de s'investir au profit des grands enjeux d'avenir qui animent notre pays.

Citoyenneté, **défense**, **sécurité nationale**, **souveraineté** ou encore **relations internationales** sont autant de thématiques sur lesquelles la jeunesse peut **faire émerger des solutions concrètes et durables**. Cela passe par la sensibilisation du plus grand nombre et c'est là que tout réside : l'Engagement.

Propulser l'en

Passerelle entre les l'association offre transformer vos idé

Développer l

Chaque année, l'a conférences, atelie techniques en prise

Que vous souhaitiez pro développement, tout est

NOS ACTIONS

0 cadres, 14 comités d'études, 2000 membres, une équipe média dédiée : c'est l'envergure d'une association ynamique qui repose sur quatre objectifs :

ngagement !

mondes civil, diplomatique et militaire, de nombreuses opportunités de ées en engagement concret.

Promouvoir l'expertise innovante

Articles, revues spécialisées, rapports d'étude, veilles : chaque année, ce sont 80 publications qui sont rédigées par nos membres et mises en valeur.

a connaissance

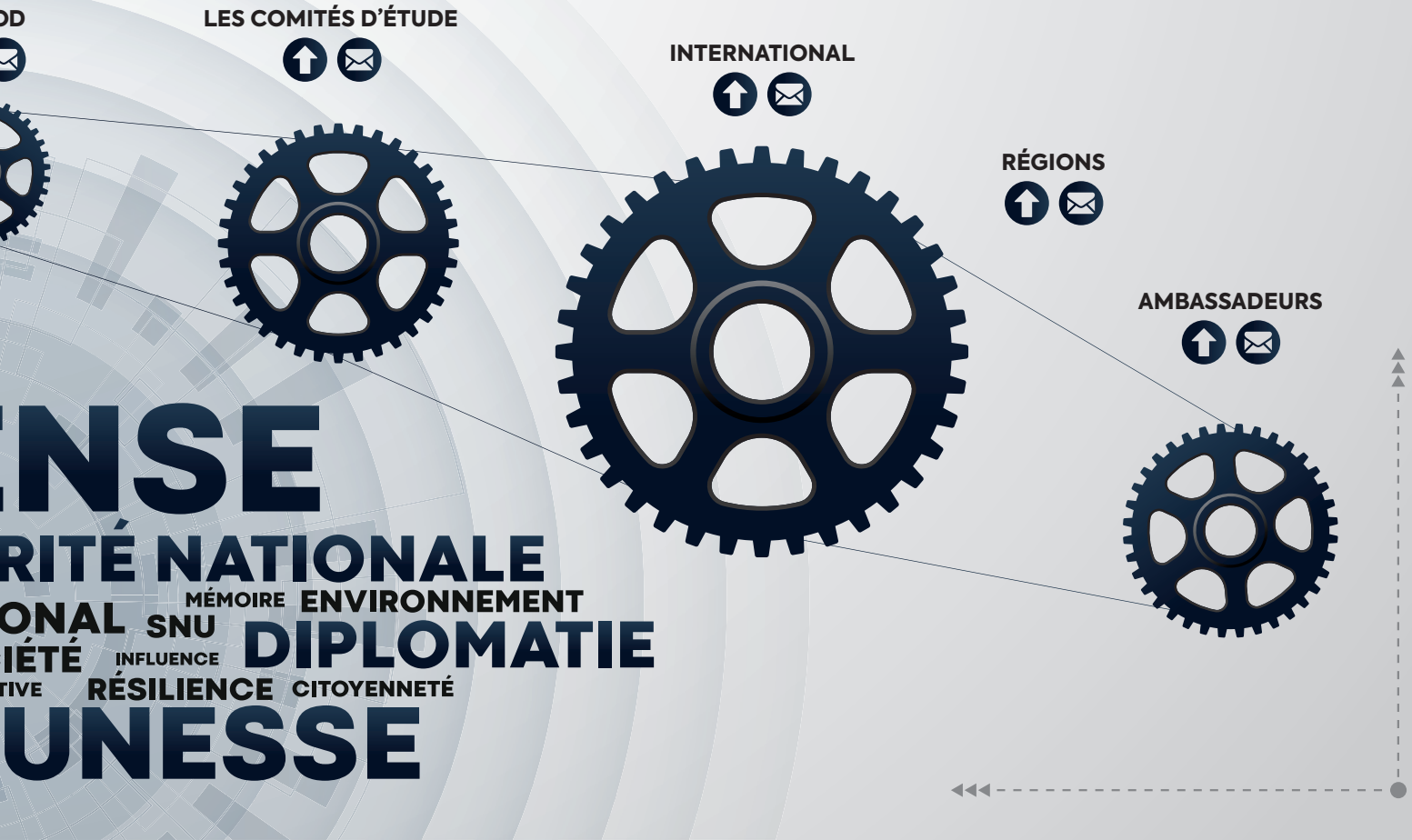
association organise une centaine de rs et visites sur des sujets généralistes ou e avec l'actualité.

Fédérer un réseau international

Étudiants, universitaires, chercheurs, jeunes professionnels, fonctionnaires, militaires ou salariés du secteur privé, le réseau des Jeunes IHEDN est riche de sa variété.

NOTRE ORGANISATION

ofiter des nombreux événements organisés par l'association, participer à ses actions ou soutenir son possible ! Il vous suffit de prendre contact ou d'aller sur le site jeunes-ihedn.org.



EXPLORE Rise MORE

FORMATIONS EN PRÉSENTIEL, DISTANCIEL OU E-LEARNING

Cette offre de formation est éligible à MON COMPTE FORMATION
moncompteformation.gouv.fr

- FORMATIONS DIPLÔMANTES ET VAE
- FORMATIONS CERTIFIANTES
- FORMATIONS SUR-MESURE

Management et leadership, Gestion, Finance, Marketing, Commercial, Entrepreneuriat, ...

Traduction : Explorez, élevez-vous plus - École historique, esprit jeune - *Compte Personnel de Formation

EM NORMANDIE
EXECUTIVE EDUCATION

OLD SCHOOL · YOUNG MIND

À travers les programmes de formations diplômantes, qualifiantes et certifiantes de l'EM Normandie, en présentiel ou à distance, salariés et dirigeants obtiendront les clés pour fixer le cap vers la réussite et amener leur carrière à bon port.

AACSB ACCREDITED · EQUIS ACCREDITED · QUALIOPI

CAEN · LE HAVRE · PARIS · DUBLIN · OXFORD

em-normandie.com/fr/formation-continue

Fondée en 1871 parmi les premières Grandes Écoles de commerce françaises, l'EM Normandie s'est imposée comme une institution de référence dans le monde des Business Schools. Elle détient les accréditations internationales EQUIS et AACSB. Avec plus de 5 000 étudiants et professionnels dans ses programmes de formations initiales et continues diplômantes et 20 000 membres de l'association Alumni EM Normandie à travers le monde, l'École est implantée sur cinq campus, à Caen, Le Havre, Paris, Oxford et Dublin. L'EM Normandie forme les managers de demain, futurs gouvernants responsables préparés à la conduite du changement dans un environnement multiculturel, et elle accompagne les salariés et dirigeants d'entreprises tout au long de leur carrière.

ENSEIGNEMENTS ET RECHERCHE : L'EM NORMANDIE S'EMPARE DE LA PROBLÉMATIQUE DE CYBERSÉCURITÉ

À travers des matières électives, des enseignements généralistes, une spécialisation dédiée, *Information System Management*, accessible en dernière année du Programme Grande Ecole (PGE) et en 3e cycle, l'EM Normandie sensibilise et forme ses étudiants aux enjeux de la cybersécurité. Elle a également lancé, à la rentrée 2020, un nouveau module Management de l'Information et des Technologies au sein de son PGE, visant à donner les clés aux étudiants pour évoluer dans un environnement tech et digital avec, notamment, un premier niveau de connaissances en cybersécurité.

Côté recherche, plusieurs enseignants-chercheurs de la Business School abordent la thématique de la cybersécurité dans leurs travaux : *« Les risques maritimes : d'Ulysse aux cyber pirates »*, *« Cybersécurité et navires sans équipage »*, *« Cybersécurité : la piqûre de rappel de l'attaque contre la ville de Baltimore »*. Ils interviennent également dans le cadre de colloques académiques, organisés par des structures externes ou par l'École en lien avec le territoire normand et les acteurs institutionnels (ANSSI, gendarmerie Nationale, …) : *« La digitalisation des ports au service de la fluidité du commerce international »*, *« Blockchains & Commerce international »*, *« Le cadre juridique de la cybersécurité »*, *« Blockchain & logistique portuaire, du conteneur physique au conteneur virtuel »*.

L'EM Normandie ambitionne, par ailleurs, de créer, en lien avec sa Fondation, une chaire *« Économie maritime et Supply Chain Management »*. Rattachée à l'axe de recherche Logistique Terre Mer Risque de son laboratoire Métis, elle se veut être un groupe d'échanges et d'expertises entre enseignants-chercheurs et professionnels pour accompagner les nouveaux challenges de la filière maritime et logistique : croissance des transports internationaux, adaptation des outils à l'augmentation des flux de marchandises, enjeux énergétiques, révolution des systèmes d'information et cybersécurité, etc.

« LE HAVRE SMART PORT CITY » AU SERVICE DE LA TRANSFORMATION DU TERRITOIRE

L'EM Normandie fait naturellement partie des nombreux acteurs locaux investis dans le projet « Le Havre Smart Port City », une démarche globale d'appui à l'innovation territoriale porté par Le Havre Seine Métropole et HAROPA Port du Havre. Son nouveau site havrais, situé au cœur du campus Le Havre Normandie et tourné vers le large, les quais et le port de plaisance et, par extension, les acteurs portuaires, est devenu aujourd'hui un emblème de la dynamique « Le Havre Smart Port City ».

POUR EN SAVOIR +
em-normandie.com

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

QUALITÉ, EXPERTISE, CONFIANCE: EXPERTCYBER, LE LABEL DE CYBERMALVEILLANCE.GOUV.FR

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

La professionnalisation et la complexité des cyberattaques impliquent la nécessité d'un accompagnement adapté des publics par des professionnels de confiance. Afin de garantir un accompagnement de qualité et d'offrir une meilleure lisibilité des prestations et services aux victimes, **Cybermalveillance.gouv.fr lance un label reconnaissant l'expertise numérique des professionnels.**

1 QU'EST-CE QUE LE LABEL EXPERTCYBER ?

Le label ExpertCyber est destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les **domaines de l'assistance et de l'accompagnement de leurs clients.**

Développé par Cybermalveillance.gouv.fr, en partenariat avec les principaux syndicats professionnels du secteur (Fédération EBEN, Cinov Numérique, Syntec Numérique), la Fédération Française de l'Assurance et le soutien de l'AFNOR, il couvre les domaines suivants :

- **systèmes d'informations professionnels** (serveurs, messageries, logiciels bureautiques…) ;
- **téléphonie** (serveurs téléphoniques professionnels) ;
- **sites Internet** (administration et protection).

Cybermalveillance.gouv.fr est le **dispositif gouvernemental de sensibilisation aux risques** numériques **et d'assistance aux victimes** d'actes de cybermalveillance

Ses publics sont les particuliers, les entreprises et les collectivités. En 2019, plus de 90 000 victimes sont venues chercher de l'assistance sur la plateforme (28 850 en 2018).

2 QUI PEUT ÊTRE LABELLISÉ ?

Peuvent être éligibles à la labellisation, les entreprises de service informatique **de toute taille**, justifiant d'une **expertise en sécurité numérique**, adressant une **cible professionnelle** et assurant des prestations d'installation, de maintenance et d'assistance.

POUR PLUS D'INFORMATIONS SUR LE LABEL EXPERTCYBER, CONTACTEZ-NOUS :
CANDIDAT@EXPERTCYBER.FR

3 POURQUOI SE FAIRE LABELLISER ?

Candidater pour le label ExpertCyber permet au professionnel d'évaluer son expertise, ses bonnes pratiques et connaissances jugées nécessaires pour remplir ses missions auprès de ses clients.

Le professionnel labellisé peut alors :
- valoriser son **expertise** ;
- offrir des **garanties** à ses clients ;
- s'intégrer dans une **communauté d'experts** ;
- apporter une expertise **sur l'ensemble du territoire** au plus près de ses clients.

Chaque professionnel labellisé est mis en avant sur la plateforme www.cybermalveillance.gouv.fr.

CÔTÉ **VICTIMES**

Le fait d'être labellisé est une garantie pour les clients. Les victimes d'actes de cybermalveillance qui choisissent de s'adresser à un professionnel labellisé peuvent attendre :
- un niveau d'expertise et de compétence en sécurité numérique ;
- un conseil de qualité pour prévenir la survenue d'autres actes de cybermalveillance et sécuriser leurs installations informatiques.

4 COMMENT SE FAIRE LABELLISER ?

La plateforme de labellisation est accessible sur : expertcyber.fr

Modalités de candidature
Le candidat devra produire des documents attestant de ses compétences et de l'organisation de ses actions d'assistance afin de justifier l'ensemble des critères à satisfaire.

La procédure sera complétée par un questionnaire technique à remplir.

Le dossier de candidature sera ensuite évalué par un auditeur de l'AFNOR et le résultat communiqué dans un délai indicatif d'un mois.

Tarif de la labellisation : 800 € HT

Durée de validité : 2 ans

AVANTDECLIQUER.COM

L'humain au coeur de la cybersécurité

Société : Avant de Cliquer
Adresse : 9, rue Georges Braque, 76000 ROUEN
Tel : 02 78 77 53 86
Site Web : **avantdecliquer.com**
Mail : **contact@avantdecliquer.com**

Spécialisations :

Avant de Cliquer permet aux DSI, RSSI, DPO et dirigeants de réduire le risque de cyberattaque de manière drastique à l'aide d'un programme de sensibilisation au phishing basé sur l'apprentissage par l'action, créé sur mesure pour chaque utilisateur et animé sur la durée. Tout cela en autopilote.

Impact :

Plus de 100 000 utilisateurs actuellement sensibilisés.

Chiffres clés :

Effectifs : 15

Historique :

Création en 2017

Dirigeant
Carl HERNANDEZ
CEO
carl@avantdecliquer.com
Tél : 02 78 77 53 86

Offres

Demandez votre audit gratuit et sans obligation d'achat, sur **avantdecliquer.com/demo**.
L'audit n'est pas réalisé sur 1 seule journée mais sur 7 jours glissants.

Conçu, créé et hébergé en France

Pour en finir avec le phishing !

Confrontez vos utilisateurs à la problématique du phishing en toute sécurité
Développez leur vigilance - Gagnez en sérénité

Sensibilisation en continu

• Parce que le mode opératoire des fraudeurs évolue, les simulations de phishing ne sont donc pas faites sous la forme de campagnes ponctuelles mais d'envois constants, ce qui est bien plus efficace.
• Parce que les fraudeurs ne préviennent pas, à chaque instant, chaque utilisateur est susceptible de recevoir un mail malveillant.

Personnalisation de l'apprentissage

Les utilisateurs peu vigilants sont sensibilisés autant de fois que nécessaire jusqu'à ce que chaque point de faiblesse détecté soit comblé.

Des mises en situation

Les mises en situation peuvent prendre plusieurs formes :

- mails comportant des liens
- capture du mot de passe dans un formulaire
- mails invitant l'utilisateur à répondre
- attaques par rebond
- SMS
- pièces jointes
- clé USB…

Amélioration des remontées d'information de vos utilisateurs

• En 1 clic, à l'aide d'un bouton "Alerte Phishing", intégré au client mail, vos utilisateurs signalent tout mail douteux.
• Le mail potentiellement frauduleux est automatiquement transmis pour analyse à votre équipe informatique.
• L'utilisateur est félicité pour son comportement positif.
• Des statistiques vous permettent de constater que le nombre de sentinelles présentes parmi vos utilisateurs augmente.

Documentation des actions mises en place

Les actions de sensibilisation menées, les améliorations constatées, les axes de progression sont documentés. Ces actions sont conformes à l'article 32 du RGPD, imposant la mise en place de mesures organisationnelles de protection des données personnelles.

E-learning

Sensibilisation initiale, couvrant des éléments de contexte et techniques liés à l'hameçonnage (30 minutes sous forme de 15 modules).
10 vidéos de 2 à 9 minutes abordant d'autres aspects de la cybersécurité.

Vous n'avez rien à faire. Tout est automatique.

Les envois ciblés sont réalisés sans action de votre part : vous n'avez pas à créer ou choisir des templates, à planifier des envois, à analyser les résultats pour sensibiliser les utilisateurs qui en ont le plus besoin.

Un accompagnement personnalisé

Chaque mois vous échangez avec un spécialiste sur les améliorations constatées et les axes de progrès, les menaces actuelles, de nouveaux modules d'e-learning et supports de communication personnalisés.

Mis en avant par Bpifrance Université — Prix de l'intelligence économique AREA — Finaliste Prix de l'innovation du SMCL 2019

PRÉSENTATION DU CYBERCERCLE

Missions / Vocation

Le CyberCercle est un cercle de réflexion créé en 2012 alors que la sécurité numérique – la cybersécurité - n'en était encore qu'à ses débuts pour de trop nombreuses organisations, et l'apanage d'un nombre encore limité d'experts techniques.

Convaincu que la sécurité et la confiance numériques ne pourront progresser qu'à la condition d'œuvrer collectivement, le CyberCercle s'est fixé 5 objectifs :

- Être un cadre privilégié d'échanges sur les questions de confiance et sécurité numériques,
- Être une plateforme de collaboration Public-Privé réunissant l'ensemble des parties prenantes,
- Décrypter le cadre réglementaire et les politiques publiques de sécurité et confiance numériques,
- Être une force de propositions pour accompagner la réflexion et le travail des parlementaires et des élus locaux sur ces questions,
- Favoriser le développement d'une culture de sécurité numérique, au delà de la sphère des experts techniques.

> **Agir efficacement ensemble pour construire une culture de sécurité numérique partagée.**

La sécurité et la confiance numériques ne constituent pas une finalité en soi mais un ensemble de disciplines et d'expertises à réunir aux services des métiers.
Dans cette perspective, le CyberCercle traite de sujets sectoriels avec une forte expertise dans les domaines de la santé, du maritime, des territoires, des collectivités, de la Défense et de sujets thématiques tels que la réglementation, l'innovation et la recherche, la formation, l'industrie 4.0...

Enfin, pour compléter cette vision « 360° » et traiter l'ensemble des dimensions stratégiques de la sécurité et de la confiance numériques, le CyberCercle a engagé des actions à l'échelon territorial avec, en 2019, un renforcement de sa présence et de son action au sein des territoires, engagé depuis 2015.

PRÉSENTATION DU CYBERCERCLE

Valeurs

Si la sécurité numérique représente un marché en tant que tel, ce qui montre son utilité économique et sa meilleure prise en compte par les organisations, il ne faut pas perdre de vue que la sécurité et la confiance numériques sont, avant toute chose, des enjeux de développement, de sécurité et de souveraineté, que ce soit au niveau national, européen et territorial.

Ce sont ces dimensions fondamentales, au service de tous, qui animent l'action du CyberCercle dont la philosophie s'appuie sur des valeurs d'engagement, de confiance, de sens du collectif et d'éthique.

Activités

Les activités du CyberCercle s'articulent autour de matinales, journées de rencontres, publications et modules de formation, déclinant un programme thématique établi chaque année.

En 2019, ce schéma directeur s'est construit autour de 3 thèmes principaux :

- Confiance numérique et politiques publiques aux niveaux national et européen : petits- déjeuners-débats-mensuels et RPCyber,
- Confiance numérique des territoires : Tour de France de la Cybersécurité (TDFCyber)
- Confiance numérique et maritime : des étapes du TDFCyber et les RPCyberMaritime.

Ces travaux se sont appuyés sur différentes publications et modules de formation.

Positionnement

Le CyberCercle a un positionnement unique.

Il est à la fois un « think tank » par la production de contenus, réflexions et propositions issus de travaux collectifs, par la diffusion d'analyses de personnalités, et par son travail d'animation de communautés ; et un créateur-organisateur d'événements fédérateurs pour :

- diffuser les éléments d'acculturation à la sécurité numérique sur l'ensemble du territoire,
- favoriser la compréhension et l'adhésion au travail parlementaire,
- devenir un acteur du conseil et de la formation pour accompagner les infrastructures dans leur réflexion en matière de politique interne de sécurité numérique,
- constituer un cadre d'influence vis-à-vis des pouvoirs publics.

Le CyberCercle est ainsi un cadre de confiance œuvrant sur des sujets d'intérêt collectif, ainsi qu'une entité fédératrice de nombreuses associations et organisations publiques et privées.

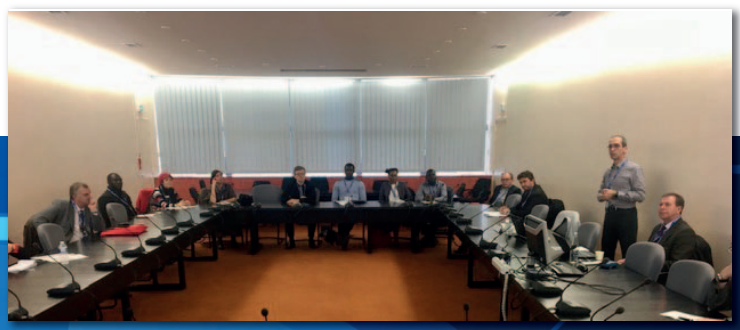
Le CyberCercle a souvent été précurseur, parfois suivi ou imité, ce qui est sans nul doute le signe qu'il œuvre dans la bonne direction, dans ce domaine où les certitudes sont peu nombreuses et souvent trompeuses, domaine qui demande en permanence d'être à l'écoute, de s'adapter, de réagir, mais toujours au service des acteurs, décideurs, métiers, et de l'intérêt général.

Entre 2012 et 2018 le CyberCercle c'était :
- 72 petits-déjeuners-débats,
- + de 600 intervenants,
- + de 9000 participants

Quelques chiffres

En 2019, le CyberCercle a réalisé :
- 11 petits-déjeuners-débats,
- 6 étapes du Tour de France de la Cybersécurité,
- 2 matinales de rencontres (7ème RPCyber - 5ème RPCyberMaritime),
- Plusieurs interventions en Outre-Mer et à l'étranger.

Pour ce faire, il a mobilisé :
- 70 partenaires, sponsors et soutiens,
- un comité stratégique composé de 16 senior advisors,
- plus de 2300 participants [1] sur l'année,
- 250 intervenants de haut niveau,
- un réseau de plus de 10 000 contacts,
- un compte Twitter réunissant plus de 8300 followers



[1] Participants uniques, venus pour beaucoup à plusieurs événements

MERCI À NOS PARTENAIRES

CYBER CERCLE