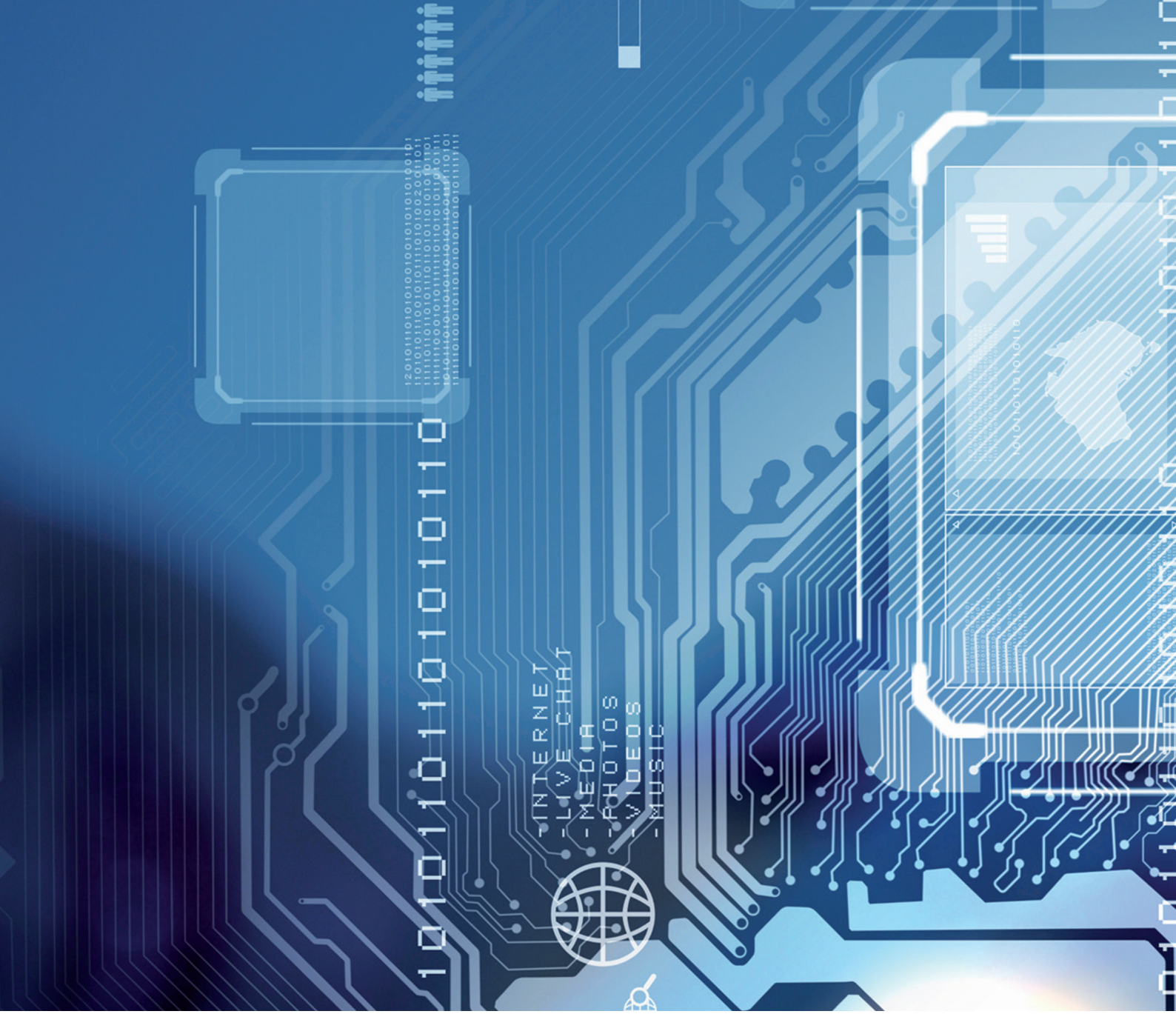


3E RENCONTRES PARLEMENTAIRES DE LA CYBERSÉCURITÉ

21 octobre 2015 - Ecole militaire, Paris

CYBER CERCLE

La dimension industrielle de la stratégie nationale pour la sécurité du numérique

/ ESPACE DE RENCONTRES - ATELIERS -DEMONSTRATIONS

OUVERT DE 8H15 À 17H

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

AIRBUS DEFENCE AND SPACE

POLE JUDICIAIRE DE LA GENDARMERIE NATIONALE (PJGN)

C3N

Département informatique électronique

Observatoire central des systèmes de transport intelligents

COFELY INEO GDF SUEZ

CENTRE D'ANALYSE DE LUTTE INFORMATIQUE DÉFENSIVE (CALID)

TREND MICRO Micro

DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA)

BRIGADE D'ENQUETES SUR LES FRAUDES AUX TECHNOLOGIES DE L'INFORMATION (BEFTI)

CROSSING SKILLS

RÉSERVE CITOYENNE CYBERDÉFENSE (RCC)

/ ET AUSSI :

IHEDN - LE SOMMET IES - LE CERCLE K2 - LE TROMBINOSCOPE - EUROSAE

DANS LES SALLES MODULAIRES DU CENTRE DE CONFÉRENCE JOFFRE

- 14H30-17H00 : Les démonstrations de SERIOUS GAMES
  Attaques ciblées de Trend Micro / Keep it safe de Layer Cake / Info Sentinel de Getzem / Cyberstrategia de la Réserve Citoyenne Cyberdéfense
- Les RENDEZ-VOUS ONE-TO-ONE avec la DGA et l'ANSSI, pour les entreprises développant des produits et des services de cybersécurité, ou faisant appel aux NTIC

8H45 : MOT D'ACCUEIL PAR BÉNÉDICTE PILLIET, DIRECTEUR DU CYBERCERCLE

9H-10H45 : SÉCURISER LE TISSU INDUSTRIEL NATIONAL

Présidée par Francis HILLMEYER, député du Haut-Rhin, et Eduardo RIHAN CYPEL, député de Seine-et-Marne

- Laurent BERNAT, Administrateur à la Division des politiques de l'information, de l'informatique et des consommateurs, OCDE
- Jean-Baptiste CARPENTIER, Délégué interministériel à l'Intelligence économique, D2IE
- Pierre GACHON, Directeur de la sécurité informatique, Groupe Renault, membre du CESIN
- Loïc GUEZO, Strategic business development and cybersecurity strategist, Trend Micro France
- Jean-Yves LATOURNERIE, Préfet, conseiller du Gouvernement, chargé de la lutte contre les cybermenaces, ministère de l'Intérieur
- Francois LAVASTE, Président, Airbus Defence & Space - CyberSecurity
- Jean-Yves POICHOTTE, Digital security director, Sanofi, membre du CESIN
- Guillaume POUPARD, Directeur général, ANSSI
- Michel VAN DEN BERGHE, Directeur général, Orange Cyberdéfense

11H00 : TÉMOIGNAGE

- Victor ROCARIES, Directeur général délégué de France Médias Monde

11H15-13H : RENFORCER LA FILIÈRE DE CYBERSÉCURITÉ DE CONFIANCE

Présidée par Gwendal ROUILLARD, député du Morbihan

- Thierry DELVILLE, Délégué ministériel aux industries de sécurité, DMIS, ministère de l'Intérieur
- Loïc DUFLOT, Sous directeur réseaux et usages numériques, ministère de l'Economie, de l'Industrie et du Numérique
- Thomas FILLAUD, Responsable du bureau Politique industrielle, ANSSI
- Jérome NOTIN, Dirigeant, Nov'IT
- Patrick RADJA, head of Cyber Defence France, Airbus Defence & Space - CyberSecurity
- Thierry ROUQUET, Président de la commission de cybersécurité, AFDEL
- ICA Frédéric VALETTE, Responsable du pôle sécurité des systèmes d'information, DGA
- Apolline AIGUEPERSE, analyste en cybersécurité, CybelAngel

13H-14H30 : DÉJEUNER (PAVILLON JOFFRE PRIVATISÉ DE 13H À 14H)

14H30 : INTERVENTION

- Vice-amiral Arnaud COUSTILLIERE, Officier Général Cyberdéfense, Etat-major des armées

14H45-17H : MASTER-CLASS

RENFORCER LA CYBERSÉCURITÉ D'UNE ENTREPRISE*

Présidée par Jean-Marie BOCKEL, ancien ministre, sénateur du Haut-Rhin

Ouverture par Philippe VERDIER, Directeur Sécurité globale, Groupe La Poste

- Colonel Philippe BAUDOIN, Coordinateur pour les cybermenaces, cabinet du DGGN
- Maître François COUPEZ, Avocat à la Cour, Atipic Avocat
- Cyrille TESSER, Coordonnateur secteur de l'industrie et des observatoires de zones SSI (OZSSI), ANSSI
- Thibault RENARD, Responsable intelligence économique, CCI France
- Sylvie SANCHIS, Comissaire de Police, Chef de la BEFTI, Préfecture de Police de Paris
- Sébastien VINANT, Directeur des offres et de l'intégration, Ineo Digital
- Représentant de la DGSI

- **Francis HILLMEYER**, député du Haut-Rhin

Né le 9 septembre 1946 à Mulhouse (Haut-Rhin), Francis HILLMEYER a une carrière de journaliste professionnel, reporter photographe. Membre du Conseil municipal de 1983 à 1989 de Pfastatt, puis adjoint au maire de 1989 à 1995, il devient maire de Pfastatt en 1995 , poste pour lequel il a toujours été réélu depuis. En 2000 il est élu député de la 6ème circonscription du Haut-Rhin, réélu depuis sans interruption. En 2006 il est élu Secrétaire de l'Assemblée nationale par ses pairs. A l'Assemblée Nationale, Francis HILLMEYER est un des piliers de la Commission de la Défense nationale et des Forces armées, à laquelle il siège depuis plusieurs législatures. Il est aujourd'hui membre des missions d'information sur l'évolution et les perspectives des dispositifs citoyens du ministère de la Défense, et sur l'évolution et le rôle de l'OTAN. Il est par ailleurs Co-président du groupe d'études Industrie aéronautique. Il a également fait partie de la Mission d'information sur les circonstances entourant l'attentat de Karachi. Francis HILLMEYER est membre titulaire de la Délégation française à l'Assemblée parlementaire de l'OTAN et de l'OSCE. Auditeur de la 56ème session de l'Institut des Hautes Etudes de la Défense Nationale (IHEDN), il est Capitaine de vaisseau dans la Réserve Citoyenne de la Marine, il est également membre de la Réserve Citoyenne Cyberdéfense.

- **Eduardo RIHAN CYPEL**, député de Seine-et-Marne

Né au Brésil en 1975, Eduardo RIHAN CYPEL arrive en France à l'âge de 10 ans, et est naturalisé en 1998. Philosophe de formation (Maîtrise de Philosophie à l'UPEC), il est diplômé de Sciences-Po Paris. Eduardo RIHAN CYPEL est élu conseiller municipal de Torcy en mars 2008, puis conseiller régional d'Ile-de-France lors des élections régionales de 2010 sur la liste de Jean-Paul HUCHON. En juin 2012, il est élu député de la 8ème circonscription de Seine-et-Marne et siège au sein de la commission de la Défense nationale et des forces armées, où il travaille particulièrement sur les questions de cyberdéfense et de cybersécurité. Il a participé à la commission du Livre Blanc sur la défense et la sécurité nationale de 2013. Eduardo RIHAN CYPEL est également Président du groupe d'amitié France-Brésil à l'Assemblée nationale.

- **Laurent BERNAT**, Administrateur à la Division des Politiques de l'Economie Numérique, OCDE

Laurent BERNAT est analyste pour l'OCDE. Il travaille notamment sur la cybersécurité et les risques d'atteinte à la vie privée qui y sont liés. Ses travaux précédents, à la Division des politiques de l'information, de l'informatique et des consommateurs de l'OCDE, soutenaient les activités du Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP/WPISP) et du Comité pour les politiques de l'informatique, de l'information et de la communication (PIIC/ICCP). Il a été en charge de la révision des Lignes directrices de l'OCDE sur la sécurité des systèmes d'information et des réseaux de 2002 et a piloté un projet pour le développement d'indicateurs statistiques sur le risque numérique. Ces dernières années, il a travaillé, en outre, sur les stratégies nationales de cybersécurité, la protection des infrastructures d'information critiques, les politiques publiques pour l'identité numérique, et la protection des enfants sur Internet. Avant de rejoindre l'OCDE en 2003, il fut chargé de mission à la Commission nationale de l'informatique et des libertés (CNIL) et directeur associé d'une agence spécialisée dans la stratégie Internet. Laurent BERNAT est titulaire d'un DEA de sciences politiques et diplômé de l'Institut d'études des relations internationales (ILERI, Paris).

- **Jean-Baptiste CARPENTIER**, Délégué interministériel à l'intelligence économique

Jean-Baptiste CARPENTIER a été nommé en Conseil des ministres du 1er juillet 2015 Délégué interministériel à l'intelligence économique.
Magistrat de l'ordre judiciaire de 1990 à 2003. Il est nommé inspecteur des Finances en 2003 et rejoint le cabinet du ministre de l'Économie, des Finances et de l'Industrie en mai 2005, en qualité de conseiller juridique, puis la Direction générale du Trésor (pôle juridique de l'Agence des Participations de l'État) en 2007.
Il a dirigé la cellule Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) de septembre 2008 à juillet 2015.

- **Pierre GACHON**, Directeur de la sécurité informatique, Groupe Renault

- **Loic GUÉZO**, Strategic Business Development and Cybersecurity Strategist, Trend Micro France

Loïc GUEZO est Directeur du développement chez Trend Micro, spécialiste japonais de cybersécurité. Il supervise le développement stratégique de Trend Micro auprès de ses clients et de ses partenaires institutionnels et gouvernementaux dans la zone Europe du Sud. En France il assure notamment l'interface avec l'ANSSI, le ministère de la Défense et la ministère de l'Intérieur. Membre du Cercle Européen de la Sécurité, il intervient auprès des médias en tant qu'expert et représente l'entreprise au sein de l'écosystème, notamment pour la France auprès du CLUSIF (Club de la Sécurité de l'Information Français, dont il est administrateur), du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) ou de l'ISA-France (pour les aspects de cybersécurité en environnement industriel SCADA). Il est également membre de l'ARCSI. Loïc GUEZO a débuté sa carrière en 1988 chez Sagem Sécurité en tant qu'Ingénieur d'étude Cryptographique pour l'OTAN. Avant de rejoindre Trend Micro en 2013, Loïc était Directeur Technique (CTO) de la division «Services de Sécurité» d'IBM France depuis 2001.

- **Jean-Yves LATOURNERIE**,Préfet, conseiller du Gouvernement, en charge de la lutte contre les cybermenaces, ministère de l'Intérieur

Ancien élève de l'École nationale d'administration (ENA - promotion Denis Diderot), le Préfet Jean-Yves LATOURNERIE est également ingénieur diplômé de l'École nationale des travaux publics de l'État (ENTPE).
Il a effectué toute sa carrière dans le secteur public, exerçant des responsabilités au sein de l'administration préfectorale, dans plusieurs administrations centrales, en collectivité locale et à la direction d'un établissement public. Il a notamment été directeur du Conseil national des activités privées de sécurité (décembre 2011), directeur général des services de la communauté urbaine de Lyon (mars 2009) et membre du Conseil supérieur de l'administration territoriale de l'État (mars 2007). Entre 2001 et 2005, il a également été directeur des systèmes d'information et de communication du ministère de l'Intérieur. Il est chevalier de la Légion d'honneur et officier de l'Ordre national du mérite.

- **François LAVASTE,** Président, Airbus Defence & Space - CyberSecurity

François LAVASTE est diplômé de l'ESCP-Europe et titulaire d'un MBA de la Harvard Business School. Après une longue carrière dans l'IT security, débutée en 1992 aux Etats-Unis, François prend la direction du comité directeur de Netasq début 2007. Netasq et Arkoon fusionnent en 2014 au sein de Stormahsield, sous la direction de François. Durant l'été 2015, François LAVASTE est nommé Président de l'entité CyberSecurity au sein d'Airbus Defence and Space.

- **Jean-Yves POICHOTTE**, Global Head of IS Security, Sanofi

Jean-Yves POICHOTTE a rejoint SANOFI en septembre 2014 en tant que Directeur de la Sécurité de l'Information du Groupe. Il définit et conduit les programmes de renforcement de la sécurité numérique du Groupe, articulant exigences Réglementaires internationales et enjeux de la protection des activités sensibles.
Il précédemment été Directeur de la Sécurité de l'Information des fraudes du groupe SFR pendant 7 ans, contribuant à renforcer la résilience des réseaux de l'opérateur et la protection de la vie privée de ses clients. Ces missions l'ont amené à travailler régulièrement avec l'ANSSI et différents services de l'Etat.
Il est Auditeur de l'Institut Nationale des Hautes Etudes de la Sécurité et de la Justice (24ème session nationale). Il est diplômé de l'Ecole des hautes Etudes Industrielles (1991). Il est membre du Jury du Prix de l'Innovation des Assises de la Sécurité. Il est membre du Conseil d'Orientation et de Programme en Sécurité de Securesphere by EPITA.

- **Guillaume POUPARD**,Directeur général, ANSSI

Ancien élève de l'Ecole Polytechnique (promotion X92), ingénieur de l'armement en option recherche, Guillaume POUPARD est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques STERN à l'Ecole Normale Supérieure de Paris et soutenue en 2000. Il est également diplômé de l'enseignement supérieur en psychologie.
Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). Il rejoint en 2006 le ministère de la Défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense. Puis en novembre 2010, devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction générale de l'armement (DGA), responsable de l'expertise et de la politique technique dans le domaine de la cybersécurité. En mars 2014, il prend la tête de l'Agence nationale de la sécurité des systèmes d'information.

- **Michel VAN DEN BERGHE**, Directeur général, Orange Cyberdéfense

Michel VAN DEN BERGHE est né en 1960. Il est Directeur Général d'Orange Cyberdefense depuis le 1er juillet 2014. Il a rejoint le groupe en janvier 2014 suite au rachat d'Atheos dont il était le Président Fondateur depuis 2002.
Il est également le fondateur des Rencontres de l'Identité, de l'Audit et du Management de la Sécurité (RIAMS) qui rassemblent depuis dix ans les principaux responsables et donneurs d'ordre du domaine de la sécurité des Systèmes d'Information.
Orange Cyberdefense rassemble toute l'expertise en Cybersécurité d'Orange Business Services et compte 1 200 collaborateurs dans 220 pays.
Michel VAN DEN BERGHE est diplômé de la Faculté polytechnique de Mons. Il est de nationalité

- **Victor ROCARIES**, Directeur général délégué, France Médias Monde

Né en 1950, Victor ROCARIES a débuté sa carrière dans l'audiovisuel en 1977 à FR3 où il occupe successivement les fonctions d'assistant de Direction chargé du contrôle de gestion des stations régionales (1977-1979), assistant de Direction chargé du contrôle de la gestion de la production du programme national et de la rédaction de l'information nationale (1979-1981), administrateur responsable de la mise en place du système de contrôle de gestion et de la comptabilité analytique pour l'ensemble de France Régions 3 (1981-1984), administrateur responsable du service de la planification et de la prospective (1984-1986). Il participe ensuite à la création de La SEPT (Société d'Edition de Programmes de Télévision), préfigurant la future structure française d'ARTE, en tant que Secrétaire Général (1987-1992) et Membre du Directoire dès 1989. En 1992, Victor ROCARIES devient Directeur Général d'ARTE France. Il rejoint ARTE G.EI.E. à Strasbourg du comité de gérance, il occupe les postes de Directeur des programmes d'ARTE (1993-2005), puis de Directeur de la gestion (depuis janvier 2005). Victor Rocaries est diplômé de l'Ecole des Hautes Etudes Commerciales (promotion 1975).
Victor ROCARIES est depuis le 1er janvier 2013, Directeur général en charge du pôle ressources du groupe France Médias Monde.

- **Gwendal ROUILLARD**, député du Morbihan

Titulaire d'une maîtrise d'histoire contemporaine, Gwendal ROUILLARD, 39 ans, est député du Morbihan depuis mai 2011. Très proche de Jean-Yves Le DRIAN, il a été son attaché parlementaire et collaborateur à son cabinet de la présidence de la région Bretagne. A l'Assemblée nationale, il co-anime « Répondre à Gauche », association historique de François HOLLANDE, présidée par Stéphane Le FOLL.
Secrétaire de la commission de la Défense nationale et des Forces armées à l'Assemblée nationale, Gwendal ROUILLARD a été co-rapporteur de la mission parlementaire préparant la prochaine Loi de programmation militaire (LPM) 2014 - 2019. Il est aujourd'hui Secrétaire de la Commission de la Défense nationale et des Forces armées, et Rapporteur pour le Budget Marine. Gwendal ROUILLARD est également membre du Haut Conseil à l'Egalité entre les Femmes et les Hommes, Co-président du groupe d'Etudes sur l'Autisme au sein de l'Assemblée nationale, conseiller municipal de Lorient, Vice-président de Lorient agglomération chargé de l'enseignement supérieur, la recherche et l'innovation, et militant de l'association Glenn Hoël en faveur de l'enfance maltraitée.

- **Thierry DELVILLE**, Délégué ministériel aux industries de sécurité, ministère de l'Intérieur

Thierry DELVILLE est diplômé de l'Ecole Nationale Supérieure de Police (ENSP) de Lyon en 1994. Il devient ensuite élève inspecteur de police à l'ESIPN de Cannes Ecluse.
Après avoir été chef de Circonscription jusqu'en 1998, il devient adjoint puis chef du bureau des systèmes d'informations et des télécommunications à la direction centrale de la Sécurité Publique (DCSP), entité composée de quinze personnes. Par la suite, Thierry DELVILLE est nommé chef du Service des Technologies de la Sécurité Intérieure (STSI) et est chargé notamment de la mise en place de partenariat avec des services notamment ministériels, tels que la DGA.
En 2009, il devient Directeur des services techniques et logistiques de la Préfecture de Police de Paris et supervise 1 550 agents avec un budget de 120 M€. Depuis 2014, Thierry DELVILLE est Délégué ministériel aux industries de sécurité.

- **Loic DUFLOT**, Sous directeur réseaux et usages numériques, ministère de l'Economie, de l'Industrie et du Numérique

Loïc DUFLOT est ingénieur en chef des mines. Après onze ans passé à l'agence nationale de la sécurité des systèmes d'information où il a notamment exercé les fonctions de sous-directeur expertise, il a rejoint en juillet 2014 la direction générale des entreprises (DGE) du ministère de l'économie de l'industrie et du numérique où il occupe les fonctions de « sous-directeur réseaux et usages numériques ». Il est membre du bureau du comité de filière des industries de sécurité et est responsable, au sein de la DGE, du suivi de la solution confiance numérique de la nouvelle France industrielle.

- **Thomas FILLAUD,** Responsable du bureau politique industrielle, ANSSI

Thomas FILLAUD est ingénieur ISEN Toulon. Il a débuté sa carrière dans le domaine bancaire en 2002, et s'est spécialisé dans la sécurité des systèmes d'information. Il rejoint en 2006 la direction générale de l'armement où il exerce pendant six années en tant qu'architecte sécurité sur de grands programmes d'armement, notamment les systèmes navals.
Depuis 2012, Thomas FILLAUD est responsable du bureau Politique Industrielle de l'ANSSI.

- **Jérome NOTIN**, dirigeant de Nov'IT

Titulaire du DTA MACAO et diplomé de l'Institut MCA, Jérôme NOTIN est le Président de Nov'IT. Impliqué dans le monde de la sécurité et des Logiciels Libres depuis de nombreuses années, Jérôme NOTIN a en particulier participé au développement de la société INL/EdenWall Technologies, à l'origine du premier pare-feu par identité.
Jérôme NOTIN a toujours travaillé pour des sociétés innovantes et apporte aujourd'hui son expérience à la société Nov'IT, qu'il a co-fondée.

- **Patrick RADJA**, Directeur Cyber Defence France, Airbus D&S - CyberSecurity

Patrick RADJA est directeur des activités Cyber Defence chez Airbus Defence and Space - CyberSecurity. Il a débuté sa carrière en 1996 en tant que project manager chez Matra Communication. Depuis il a développé une solide expérience à travers différentes fonctions de management chez Airbus group, se spécialisant à partir de 2001 sur les activités de cyber défense. Son expérience va du développement de produits et services à leur déploiement, y compris dans le cadre de projets complexes. Il a contribué activement à la structuration de l'offre d'Airbus DS – CyberSecurity et au lancement de ses offres de produits et services.
En 2012 il a pris la tête de la direction Cyber Defence. Il est également directeur de l'ingéniérie et des opérations en France.

- **Thierry ROUQUET**, Président de la commission de cybersécurité, Association française des éditeurs de logiciels (AFDEL)

Thierry ROUQUET (56 ans) est Président et co-fondateur de Sentryo, une start-up technologique pionnière sur le marché de la protection de l'Internet Industriel contre les cyber risques qui se lance sur les marchés Français et Allemand. Il est un entrepreneur en série. Il a dirigé Arkoon Network Security, un éditeur de solutions de cyber sécurité des réseaux et des postes de travail, pendant 10 ans. Sous sa direction, la société a été introduite en bourse avant d'être acquise par la division défense et sécurité du groupe Airbus. Il avait auparavant crée Axidia une société de l'Internet cédée à l'américain Scient. Thierry ROUQUET est administrateur et président de la commission cyber sécurité de l'AFDEL, l'Association Française des Editeurs de Logiciel et Solutions Internet. Il est aussi membre du Réseau de Réserve Citoyenne de Cyberdéfense (RCC). Il est enfin associé et fondateur d'Axeleo, le premier accélérateur de start-up B2B en France soutenu par BPI dans le cadre du programme French Tech. Thierry ROUQUET est diplômé de l'INSA de Lyon.

- **ICA Frédéric VALETTE**, Responsable du pôle Sécurité des Systèmes d'Information, Direction générale de l'armement

L'ingénieur en chef de l'armement Frédéric VALETTE est depuis le 2 Avril 2014 responsable du pôle Sécurité des Systèmes d'Information à la Direction générale pour l'armement (DGA).
Après avoir réalisé pendant dix ans un travail d'expertise en cryptographie dans un premier temps à l'ANSSI puis dans le centre DGA Maitrise de l'Information, il a successivement dirigé le département de cryptologie puis la division SSI qui regroupe les quelques 200 experts du domaine au sein du centre de DGA Maitrise de l'Information.
Il est actuellement à la tête de l'ensemble des équipes techniques chargées au sein de la DGA de sécuriser les systèmes qui seront livrés aux forces et de mener une activité de R&D dans le domaine de la cyberdéfense.

- **Apolline AIGUEPERSE,** analyste cybersécurité, CybelAngel

Apolline AIGUEPERSE fait partie de l'équipe d'analystes en cybersécurité au sein de la société CybelAngel. Il s'agit d'une start-up française spécialisée dans la détection d'attaques informatiques et de fuites de données en temps réel.

Après une license et un master à Sciences Po Paris et plusieurs expériences au Ministère de la Défense, Apolline AIGUEPERSE a travaillé au sein de la NATO Communications and Information Agency (NCIA) avant de rejoindre CybelAngel.

- **Vice-amiral Arnaud COUSTILLIERE**, Officier Général Cyberdéfense, Etat-major des armées

Né à Toulon le 3 novembre 1960, la carrière du Vice-amiral COUSTILLIERE s'est essentiellement partagée entre des embarquements et commandements opérationnels sur des navires de combat, et des postes de responsabilités en administration centrale, avec une spécialisation plus particulière pour les télécommunications et la cyberdéfense. Il a été nommé officier général à la cyberdéfense le 1er juillet 2011 à la création du poste. Directement rattaché au sous-chef « opérations » de l'état-major des armées, et placé sous la double tutelle du chef d'état-major des armées et du chef de cabinet militaire du ministre, il est responsable de la cyberdéfense du ministère et de sa conduite en situation de crise cybernétique. En février 2011, en cohérence avec l'extension des missions de l'ANSSI, il avait été nommé chargé de mission cyberdéfense auprès du sous-chef « opérations » tout en conservant de façon temporaire ses fonctions précédentes. En poste à l'état-major des armées depuis l'été 2008, il a été officier de cohérence opérationnelle en charge du domaine des télécommunications et de la cyberdéfense. Issu le la promotion 1981 de l'Ecole Navale, il a été embarqué sur de nombreux bâtiments de combat et déployé en zones de crises, principalement en Méditerranée et dans le nord de l'Océan Indien. Il a exercé le commandement de la frégate lance-missiles « DUQUESNE » (2004-2006), des avisos « CDT BOUAN » (1996) et « D'ESTIENNE D'ORVES » (1995) ainsi que du bâtiment-école « CHACAL » (1987). Il a aussi occupé plusieurs postes tant à l'état-major de la Force d'Action Navale (doctrine 2004) qu'à l'état-major de la Marine (coordonnateur central CMI et chef du bureau SIC (2006), adjoint au chef du bureau Finances (2002), officier correspondant d'état-major CMI (1999), officier de programme Syracuse (1991). Le Vice-amiral Arnaud COUSTILLIERE est chevalier de la Légion d'Honneur et officier de l'ordre national du mérite. Il est titulaire de la Croix du combattant, de la médaille d'Outre-mer (Moyen Orient), de la médaille de la Défense nationale, et de différentes médailles commémoratives des théâtres d'opérations extérieures.

Intervention : Présentation du concours mondial 2016 de l'innovation (Commission Innovation 2030 et BPI) et de son nouvel axe «protection et défense contre les malveillances»

- **Jean-Marie BOCKEL**, ancien ministre, sénateur du Haut-Rhin

Après des études de droit et un diplôme d'avocat, Jean-Marie BOCKEL ouvre son cabinet d'avocat à Mulhouse en 1976, tout en débutant un engagement politique au Parti Socialiste.De 1981 à 1993, puis de 1997 à 2002, il est député du Haut-Rhin. Depuis 2004, Jean-Marie BOCKEL est sénateur du Haut-Rhin, membre de la Commission des Affaires étrangères, de la Défense, et des Forces armées du Sénat, pour laquelle il a rédigé en juillet 2012 le rapport « La Cyberdéfense : un enjeu mondial, une priorité nationale », et co-rédigé en octobre 2013 le rapport « L'Afrique est notre avenir ».
Jean-Marie BOCKEL est par ailleurs membre titulaire de l'Assemblée Parlementaire du Conseil de l'Europe. Secrétaire d'Etat auprès du ministre du commerce, de l'artisanat et du tourisme en 1984, Jean-Marie BOCKEL a été nommé ministre du commerce, de l'artisanat et du tourisme en 1986. En tant que ministre d'ouverture, il est nommé en juin 2007 Secrétaire d'Etat chargé de la coopération et de la francophonie, en 2008 Secrétaire d'Etat à la Défense et aux anciens combattants, puis en 2009 Secrétaire d'Etat à la Justice, poste qu'il assumera jusqu'en 2010. Jean-Marie BOCKEL est depuis 2010 Président de Mulhouse Alsace Agglomération, et conseiller municipal de Mulhouse - dont il a été maire de 1989 à 2010. Il a été conseiller général du Haut-Rhin pendant dix ans, conseiller régional d'Alsace en 1992, et Président de l'Association des maires des grandes villes de France de 2001 à 2007. Jean-Marie BOCKEL est colonel de réserve de l'armée de Terre (affecté à la Brigade Franco-Allemande) et membre de la Réserve Citoyenne Cyberdéfense. Il est Chevalier dans l'Ordre National de la Légion d'Honneur.

- **Philippe VERDIER**, Directeur Sécurité Globale, Groupe La Poste

Après une maîtrise d'économie et un passage au sein de l'administration fiscale, Philippe VERDIER intègre les PTT en décembre 1979 et suit la scolarité de l'Ecole Nationale des PTT de 1984 à 1987.
A l'issue de sa formation, il prend en charge au sein de la Direction Financière de La Poste le projet de mise en oeuvre d'une comptabilité d'entreprise en préparation de la création de France Télécom et de La Poste. En 1991, il prend la responsabilité du service comptable de La Poste.
En 1994, il est chargé de la création de la Direction des Systèmes d'Information du Groupe et assure à ce titre le pilotage du passage à l'an 2000 et le pilotage du projet de passage à l'euro. En 2001, il prend la responsabilité du Réseau Grand Public (direction des bureaux de poste) avec pour missions principales d'organiser les points de contact (création des points commerçants, rénovation des agences postales, regroupement des établissements dans une zone de vie) et de participer à la construction de La Banque Postale. En 2004, il est nommé Directeur Général de Sofipost puis Président de Docapost avec pour objectif de développer les filiales du Courrier notamment en termes d'intégration des services alliant processus physiques et processus numériques. Depuis 2011, Philippe VERDIER assure la direction de la Direction de la Sécurité Globale du Groupe La Poste et les fonctions d'adjoint du Délégué Général du Groupe pour les fonctions supports (télécommunications, DSI hors branches, véhicules, action sociale...).

Intervention : Définition et mise en oeuvre d'une politique de cybersécurité globale et cohérente : l'exemple du groupe La Poste

- **Colonel Philippe BAUDOIN**, Coordinateur pour les cybermenaces, chargé de mission au Cabinet du Directeur Général de la Gendarmerie Nationale

Le colonel Philippe BAUDOIN suit un parcours d'ingénieur à l'Ecole polytechnique de 1985 à 1988 puis, est diplômé en criminalistique à l'UFR de Biomédicale, à l'Université de Paris V après avoir passé une année à l'Ecole de guerre de 2001 à 2002. Il devient chef du département micro-analyse de l'Institut de recherche criminelle de la gendarmerie de 1991 à 1995. Le colonel BAUDOIN poursuit sa carrière en gendarmerie et devient chef de la division criminalistique Ingénierie & Numérique de l'IRCGN jusqu'en 2005. Par la suite, le colonel se spécialise en cybercriminalité et devient Chef de la division de lutte contre la cybercriminalité au Service Technique de Recherches Judiciaires et de Documentation jusqu'en 2008.Depuis juin 2015, il est coordinateur pour les cybermenaces, chargé de mission au cabinet du DGGN. Le colonel Philippe BAUDOIN est également officier de l'Ordre national du Mérite et Chevalier de l'Ordre nationale de la Légion d'honneur.

Intervention : Réaction face à une atteinte cyber, preuves numériques et contacts avec les forces de police

- **Maître François COUPEZ**, Avocat à la Cour, Cabinet ATIPIC Avocats

Au sein du cabinet ATIPIC dont il est associé-gérant et cofondateur, Me Coupez met sa double compétence en droit et technologies de l'information au service de nombreuses grandes entreprises afin de les conseiller et de les assister face à leurs contraintes réglementaires. Avocat à la Cour, ancien responsable du droit des nouvelles technologies du Groupe Société Générale, il est également titulaire du Certificat de spécialisation en Droit des nouvelles technologies délivré par le Conseil National des Barreaux. Il enseigne à l'Université Paris II ou encore au CELSA et intervient depuis de nombreuses années sur les problématiques juridiques de sécurité des systèmes d'information.

Intervention : Pourquoi les « chartes informatiques » sont-elles incontournables pour assurer la sécurité des systèmes d'information des entreprises ?

- **Cyrille TESSER**, Coordonnateur secteur de l'industrie et des observatoires de zones SSI (OZSSI), ANSSI

Cyrille TESSER a un DESS ainsi qu'un Master en SSI à l'Université de technologie de Troyes. Il dispose également du titre d'expert en SSI (ESSI et BESSSI) qu'il a acquis au cours d'un parcours professionnel au ministère de la Défense, de 1996 à 2013. Il a été, durant ces années, chargé d'étude, RSSI, formateur SSI et auditeur.
En plus de ses activités, il est également expert judiciaire à la Cour d'Appel de Paris depuis une dizaine d'années. A l'ANSSI depuis 20113, il coordonne le secteur de l'industrie ainsi que les observatoires de zones SSI (OZSSI).

Intervention : Panorama des moyens à votre disposition et nouvelles perspectives

- **Thibault RENARD**, Responsable Intelligence Economique - Département Industrie, Innovation, Intelligence économique, CCI France

Thibault RENARD est Responsable Intelligence Economique à CCI France, établissement national fédérateur et animateur des Chambres de Commerce et d'Industrie. Précédemment en poste à la Mission Economique de l'Ambassade de France en Autriche, il est également administrateur au syndicat Français de l'Intelligence Economique (Synfie). Titulaire d'une Maîtrise de Science Physiques et d'un DESS Intelligence Économique et Développement de l'Entreprises, il intervient par ailleurs sur l'Intelligence Economique Européenne et Territoriale en Ecoles de Commerce et d'Ingénieur.

Intervention avec **Coralie OUTREVILLE**, CCI du Cher et **Frédéric REMI**, EDEN Bretagne :
Projet d'actions collectives structurées à destination des entreprises dans les domaines de la cybersécurité : les Serious Games et retex d'EDEN

- **Sébastien VINANT**, Directeur des offres et de l'intégration, Ineo Digital

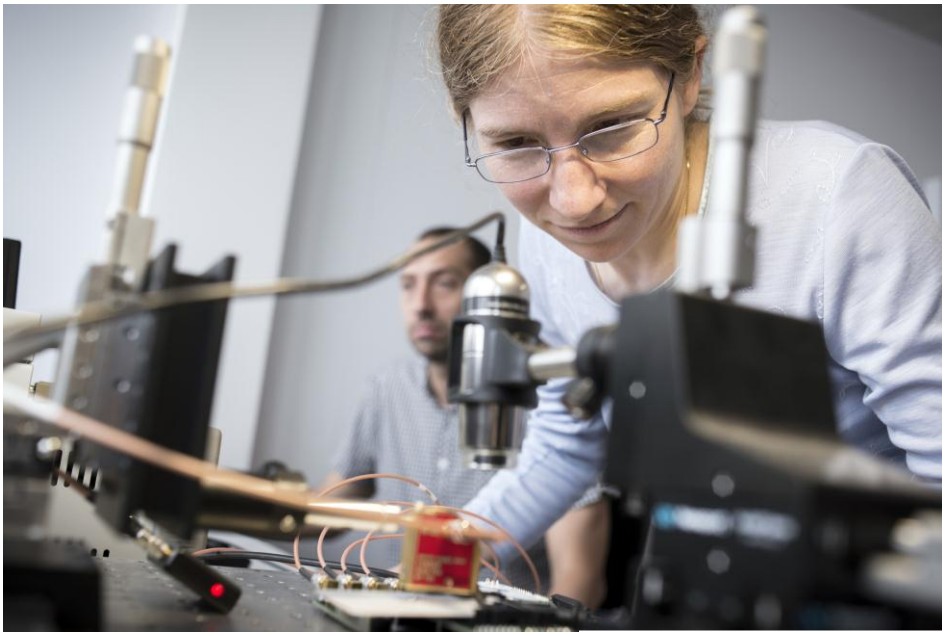
Sébastien VINANT est Directeur des offres et de l'intégration d'Ineo Digital, entité de Cofely Ineo qui développe des solutions et services innovants dans le domaine des infrastructures numériques (Communications Unifiées, Réseau, Cloud) ainsi que des solutions métiers pour les Smart Cities, Smart Building et l'e-Santé. Il est intervenu auprès de nombreuses entreprises et opérateurs de services aux collectivités sur le pilotage de projets de transformation et d'intégration de systèmes d'information.
Il a effectué une grande partie de sa carrière dans le développement des services numériques pour le secteur de l'énergie et des services aux collectivités au sein de Schlumberger Industries comme Directeur du développement, comme Senior Manager chez Atos Consulting puis comme Associate Partner chez IBM Global Business Services. Il est diplomé de l'Ecole Nationale Supérieure de Techniques Avancées.

- **Sylvie SANCHIS**, Commissaire de Police, chef de la BEFTI, Préfecture de Police
  Intervention : les piratages de standards téléphoniques

- Représentant DGSI - Intervention : Premier verrou de la sécurité informatique : le facteur humain

Qualification des produits de sécurité et des prestataires de service de confiance

La qualification est un label encadré réglementairement, délivré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui atteste de la **robustesse** et de la **confiance** d'un produit ou d'un service.



Crédit photo : Patrick Gaillardin - Picturetank

Critères de qualification : robustesse et confiance

La **robustesse** d'un produit ou d'un service est sa capacité à résister à des attaques informatiques.

Un certain niveau de **confiance** peut être accordé dans la société, ses processus de conception, de développement, de fabrication, d'exploitation, de maintenance, de livraison afin de minimiser le risque de piégeage et s'assurer que le produit ou le service puisse être utilisé en toute confiance tout le long de son cycle de vie.

Comment évaluer le niveau de robustesse et de confiance ?

Le niveau de **robustesse** d'un produit ou d'un service est évalué dans le cadre d'une expertise technique (audit technique et organisationnel, test d'intrusion, etc.) du produit ou du service.

L'évaluation du niveau de **confiance** d'un produit ou d'un service prend en compte plusieurs facteurs : analyse de la chaîne logistique, sous-traitance des tâches de conception, de fabrication, d'exploitation ou de maintenance, composition du capital de la société, etc. La réglementation permet à l'ANSSI de demander des enquêtes administratives sur les sociétés souhaitant faire qualifier leur produit ou leur service.

Retrouvez le catalogue des produits et services qualifiés sur **www.ssi.gouv.fr**

Plan Cybersécurité
de la Nouvelle France Industrielle

Lancé le 12 septembre 2013 dans le cadre de la Nouvelle France Industrielle (NFI), le plan Cybersécurité est piloté par l'ANSSI qui en assure l'animation en soutien des acteurs publics et privés de la filière.

A l'occasion du lancement de la seconde phase de la NFI par le ministre de l'économie, de l'industrie et du numérique, le 18 mai 2015, autour de l'Industrie du futur, le plan Cybersécurité a été regroupé au sein de la solution industrielle « Confiance numérique ».

Les quatre axes stratégiques

Le plan Cybersécurité comprend à ce jour quatre axes stratégiques et seize actions qui leur sont associées :

1. Accroître la demande en produits et services au niveau national
2. Développer des offres de confiance
3. Organiser la conquête des marchés à l'étranger
4. Consolider la filière cybersécurité

Les principales réalisations du plan

Un an et demi après la validation de la feuille de route par le ministre de l'économie, de l'industrie et du numérique, voici les principales réalisations issues du plan :

- la création du label *FRANCE CYBERSECURITY*, faisant aujourd'hui l'objet d'une gouvernance autonome. Après la remise des 24 premiers labels à l'occasion du FIC 2015, de nouveaux labels ont été délivrés le 16 octobre à l'issue d'une deuxième campagne de labellisation ;
- la structuration et renforcement de l'action étatique en matière de soutien à l'exportation, aujourd'hui poursuivis dans le cadre de la stratégie nationale pour la sécurité du numérique ;
- la publication, par l'ANSSI, d'un guide d'achat de produits de sécurité et de services de confiance qualifiés au profit des Administrations ;
- la définition et la publication de 16 profils métiers de la cybersécurité, destinés à améliorer le lien entre la formation et les besoins en recrutement d'experts du domaine ;
- la création récente d'un groupe de travail relatif au développement économique des entreprises de la filière.

En sus de la concrétisation des actions d'ores et déjà engagées, la promotion des règles et bonnes pratiques en matière de cybersécurité seront poursuivies au cours de l'année 2016, au sein de la solution « Confiance numérique ».

La Cyberdéfense au ministère de la Défense

Un enjeu de souveraineté, une doctrine nationale

Le Livre Blanc sur la Défense et la sécurité nationale de 2013 rappelle que la capacité de l'Etat à se protéger contre des attaques informatiques majeures constitue un élément de souveraineté nationale. Dans le cadre de la doctrine nationale de réponse aux agressions informatiques majeures, la cyberdéfense regroupe l'ensemble des actions défensives et offensives conduites dans le cyberespace. Il s'agit de pouvoir garantir le bon fonctionnement du Ministère de la Défense et l'efficacité de l'action des forces armées en préparation ou dans la planification et la conduite des opérations.

La DGA, garant de l'expertise technique en cyberdéfense

La Direction générale de l'armement (DGA) est l'expert technique référent du ministère de la Défense en matière de cybersécurité. Elle assure dans son établissement DGA Maîtrise de l'information (situé à Bruz, près de Rennes) :

- une mission d'expertise de haut niveau quant à la connaissance et à l'anticipation de la menace cyber,
- un rôle de conseil et de soutien à la lutte informatique défensive du ministère de la Défense,
- le développement et l'évaluation de produits de cybersécurité pour la défense et les hautes autorités de l'État,
- la prise en compte de la cybersécurité dans tous les programmes d'armement, jusqu'aux architectures sécurisées de systèmes complets,
- la conception de moyens de chiffrement gouvernementaux,
- l'animation et le développement de la R&T (recherche & technologie) cyber en lien avec les autres entités étatiques, l'industrie (notamment via le soutien aux entreprises innovantes) et le monde de la recherche (notamment via le financement de thèses).

Une partie de ses équipes intervient directement au profit du CALID ou de l'ANSSI pour l'analyse des attaques les plus complexes détectées sur les réseaux et des menaces potentielles les plus dangereuses.

Pour disposer d'une capacité d'expertise à la hauteur des enjeux majeurs portés par la cyberdéfense, ce sont déjà près de 300 ingénieurs de très haut niveau qui sont localisés à DGA Maîtrise de l'information, ce nombre devant être porté à 500 d'ici 2019.

L'action de la DGA en faveur des PME

En tant que premier acheteur public, la DGA a par ailleurs une responsabilité particulière dans l'objectif de l'Etat de soutenir le développement des PME : environ 11 milliards d'euros de commandes sont en effet passées chaque année à l'industrie, soit deux tiers des marchés publics

passés par l'Etat et plus du quart du montant des marchés passés par l'ensemble des administrations publiques.

Régime d'Appui à l'Innovation Duale (RAPID)

Avec une enveloppe de 50M€ en 2015 (soit une augmentation de 25% depuis 2012), RAPID concerne les projets de recherche industrielle ou de développement expérimental à fort potentiel technologique des PME et ETI (entreprises de taille intermédiaire de moins de 2000 salariés), présentant des applications militaires et ayant aussi des retombées sur les marchés civils.

Ce dispositif est conçu pour être extrêmement réactif afin d'accorder un financement aux projets sélectionnés dans un délai de quatre mois entre le dépôt du dossier et le début des travaux.

+ d'infos : www.ixarm.com/Projets-d-innovation-duale-de-PME

Le Pôle d'excellence cyber : faire converger les compétences

Le Pôle d'excellence cyber, initiative conjointe du ministère de la Défense (pacte défense cyber) et de la Région Bretagne (pacte d'avenir), a une portée nationale et un objectif de rayonnement international.

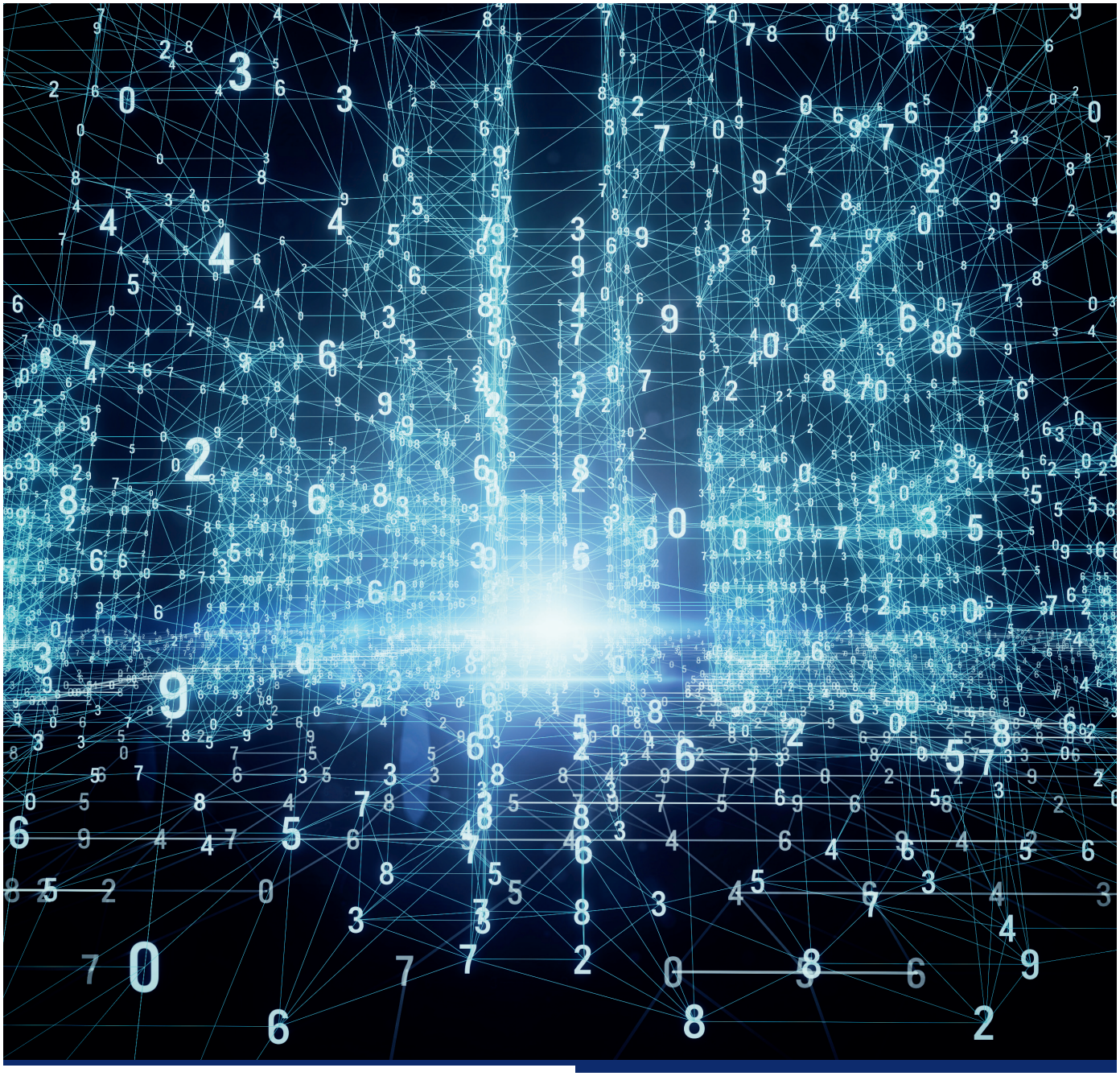
Il a pour mission de :

- développer la formation initiale, la formation continue et l'enseignement supérieur pour garantir la disponibilité des compétences nécessaires,
- stimuler la recherche et l'innovation dans le domaine cyber pour favoriser l'émergence de solutions (services et produits) de confiance,
- favoriser le développement de la filière industrielle, avec une attention particulière portée aux PME/PMI innovantes, y compris à l'export.

Concentré autour des acteurs du ministère (DGA Maîtrise de l'information, CALID Bretagne, École des transmissions, Écoles de Saint-Cyr Coëtquidan, École navale, ENSTA Bretagne), il s'appuie sur le tissu académique et industriel régional, particulièrement dense en matière de cybersécurité et de numérique, mais aussi sur des partenaires nationaux ou d'autres territoires.

Le Pôle d'excellence cyber s'appuie sur les organismes technico-opérationnels du ministère pour mettre également en place les plates-formes nécessaires à la formation, à l'entraînement et à la gestion de cyberattaques ainsi qu'à l'expérimentation de nouveaux produits de sécurité informatique.

À ce jour, le Pôle d'excellence cyber compte déjà près de 50 partenaires majeurs (publics ou privés, civils ou militaires), dont 13 grands groupes : Airbus D&S, Alcatel, Atos-Bull, Bertin, Cap Gemini Sogeti, DCI, DCNS, EDF, La Poste, Orange, Safran, Sopra-Stéria, Thales.



CyberSecurity made in Europe

PIONEERING THE FUTURE TOGETHER

AIRBUS
DEFENCE & SPACE

Airbus Defence and Space – CyberSecurity : L'EUROPE DANS NOS GÊNES

Plus de **600** experts en cyber sécurité

Plus de **20%** des revenus annuels dédiés à la R&D

3 Cyber Defence Centres en Europe, pour la protection 24/7 des actifs de nos clients

Pour faire face au défi que constitue la sécurité des systèmes d'information pour les sociétés modernes, Airbus Defence and Space (Airbus DS) a rassemblé l'ensemble de son expertise au sein d'une filiale entièrement dédiée aux activités de cyber sécurité. Avec plus de 600 experts en Europe, opérant depuis trois pays (France, Royaume-Uni, Allemagne), Airbus DS - CyberSecurity met son expertise et ses solutions européennes au service de ses clients : services gouvernementaux et de défense, infrastructures critiques et entreprises.

Partenaire de confiance des gouvernements et des forces armées, Airbus DS – CyberSecurity propose une offre de produits et de services développés en pleine cohérence avec les exigences de sécurité des autorités nationales – telles que la Loi de Programmation Militaire - , et destinées à répondre aux contraintes opérationnelles de ses clients. Nos solutions sont notamment déployées au profit des forces sur les théâtres d'opération, ainsi qu'au bénéfice des organisations privées – entreprises stratégiques, opérateurs d'importance vitale, pépites technologiques- qu'il convient d'accompagner dans la protection de leur patrimoine économique et intellectuel.

Nous sommes fiers de contribuer à la résilience de nos systèmes et donc à la survie de notre appareil économique et de nos structures sociales, grâce à un investissement constant dans nos capacités d'innovation. En effet, pour faire face à des attaques protéiformes, se jouant des frontières et démontrant un niveau de sophistication croissant, il nous faut être en mesure d'apporter sur le marché, rapidement, des solutions éprouvées, évolutives et d'excellence, tirant le meilleur des expertises de nos différents pays d'opération. C'est pourquoi nous consentons plus de 20% de notre chiffre d'affaires annuel aux investissements de recherche et développement.

La cyber sécurité est également une filière technologique d'avenir, bâtie sur un marché en pleine croissance, avec près de 20 milliards d'euros pour la seule région européenne en 2016. Nous sommes fiers de contribuer au développement d'une telle filière d'excellence, aux niveaux national et européen. En effet, seule la croissance de ce tissu technologique et économique pourra garantir la protection maîtrisée des actifs de nos sociétés et le développement d'expertises et de savoir-faire de pointe.

AIRBUS DEFENCE & SPACE

Airbus Defence and Space
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France / T: +33 (0) 1 61 38 50 00
Willy-Messerschmitt-Str. 1 / 85521 Ottobrunn / Allemagne / T: +49 (0) 89 607 - 0
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / Royaume-Uni / T: +44 (0) 16 33 71 30 00

Solutions de cybersécurité

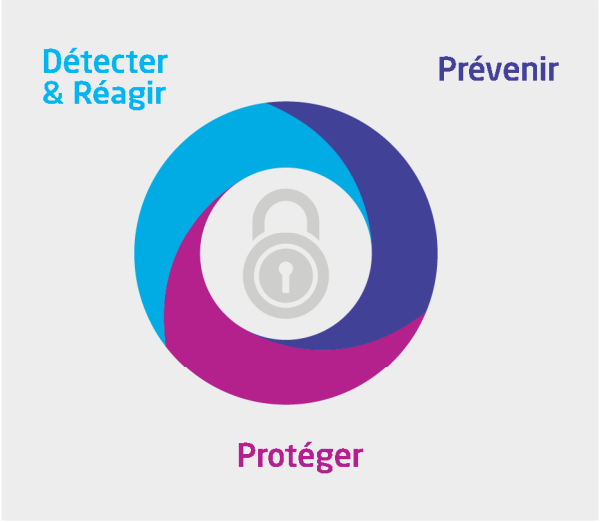
Une approche globale, des prestations adaptées, sur-mesure et complémentaires

Intégrateur de systèmes, Cofely Ineo conçoit, développe, déploie et maintient des solutions de sécurité opérationnelles à même de répondre aux enjeux de cybersécurité de ses clients.

Prévenir

Les nouveaux usages liés au numérique, associés à un renforcement du cadre réglementaire, amènent les organisations à repenser leur stratégie de cybersécurité. Cofely Ineo accompagne les acteurs privés et publics dans la définition et la mise en œuvre de processus et de moyens de prévention des cyberattaques. Ces solutions sont adaptées et efficaces, grâce à des prestations de conseil et d'audit sur mesure :

- définition des politiques de sécurité,
- analyse de risques,
- étude d'architectures sécurisées,
- organisation de la sécurité et conception des stratégies d'homologation,
- audits de sécurité.



Protéger

Le déploiement de moyens de protection adaptés permet de contrôler l'accès aux informations de l'organisation et de se prémunir contre les fuites de données.

Sécurisation des infrastructures :

- définition des politiques de sécurité du SI,
- architecture,
- réseaux de communication,
- data centers.

Sécurisation de la mobilité :

- voix & données pour tablettes et smartphones,
- partage de données dans le cloud,
- accès aux données de l'entreprise.

Détecter & Réagir

La complexité des cybermenaces a fait de la surveillance des systèmes d'information un élément essentiel dans la stratégie de cyber sécurité des organisations.

Cofely Ineo a développé des capacités avancées de maintien en condition de sécurité des systèmes, pour détecter les cyberattaques et y réagir, qui intègrent notamment :

- la veille sécurité,
- la traçabilité et l'assurance,
- l'analyse d'impact de nouvelles vulnérabilités.

Cofely Ineo propose en outre à ses clients privés la mise en oeuvre de centres opérationnels de sécurité.

COFELY INEO
GDF SUEZ
GDF SUEZ devient ENGIE

cofelyineo-gdfsuez.com

Orange Cyberdefense

Abordez votre transformation digitale en confiance

Avec la déferlante numérique et l'explosion de la cybercriminalité, les entreprises, en pleine transformation digitale, deviennent de plus en plus vulnérables.

Aujourd'hui, la question n'est plus de savoir si votre entreprise va être attaquée, mais comment s'y préparer. Il faut donc passer d'un mode préventif à un mode proactif et apprendre à se défendre face aux agresseurs en tout genre.

Orange Cyberdefense est la réponse globale d'Orange aux risques et menaces du monde digital.

notre ambition

Devenir le partenaire de confiance de votre transformation digitale.

nos convictions

- la sécurité est un facteur d'opportunité qui doit accompagner la performance et l'innovation,
- la sécurité doit être abordée de façon globale, proactive et réactive,
- tout protéger est illusoire, il faut se concentrer sur la protection des actifs sensibles et limiter l'impact des incidents inévitables,
- la souveraineté doit être une priorité.

nos 4 domaines d'intervention

Afin d'accompagner nos clients dans cette stratégie de « défense active », nous avons élaboré une réponse construite sur 4 piliers :

- définir votre stratégie de défense et l'adapter en permanence,
- assurer la protection digitale des données et des personnes clés,
- détecter les signaux faibles et anticiper la menace,
- concilier une organisation défensive structurée avec une réactivité immédiate en cas d'attaques avérées.

nos solutions phares

Pour mieux répondre aux nouveaux enjeux de ses clients, Orange Cyberdefense a développé 3 solutions innovantes :

- faire de la souveraineté une priorité : **Calypso**
  concept :
  - maîtriser l'hébergement et le traitement de vos données sur le territoire national.

  bénéfices :
  - identifier les points de faiblesse et les vulnérabilités de vos infrastructures,
  - profiter d'un environnement étanche et dédié, accessible uniquement par des personnels Orange habilités.
- prendre en compte les risques métiers et les menaces avancées : **SOC 2.0**
  concept :
  - couvrir l'ensemble des menaces, y compris avancées, liées aux infrastructures et réseaux, aux applications et aux *devices*.

  bénéfices :
  - disposer de l'expérience d'opérateur Orange grâce à la convergence entre les moyens internes et le service aux clients entreprises.
  - profiter de l'écosystème construit autour de notre SOC : laboratoire, service de veille, surveillance métier et comportementale, surveillance des personnes clés (y compris GSM), surveillance des réseaux industriels…
- observer pour devancer : **DDoS Protection**
  concept :
  - bénéficier de notre réseau d'opérateur pour effectuer une surveillance préventive depuis différentes zones géographiques sensibles,
  - mettre en œuvre des mitigations ou des contre-mesures avant le lancement de l'offensive.

  bénéfices :
  - savoir « qui attaque qui » en avance de phase,
  - être capable de se prémunir proactivement d'attaques imminentes.

nos facteurs différenciateurs

- notre approche
  - ajuster les dispositifs de défense suivant la typologie des menaces et la sensibilité des actifs,
  - capitaliser sur notre expertise historique d'opérateur d'infrastructures sensibles.
- notre positionnement
  - capacité d'accompagnement sur toutes les dimensions d'une stratégie de sécurité et de sa mise en œuvre opérationnelle,
  - acteur vertical couvrant la cybersécurité de bout en bout et multi-modèles : service intégré, managé ou hybride.
- nos moyens
  - plus de 1000 experts dédiés à la sécurité des SI,
  - présence dans 220 pays,
  - laboratoire d'épidémiologie et de veille,
  - centre d'opérations sécurisé pour les infrastructures et systèmes d'information des clients les plus sensibles,
  - 30 années d'expérience en gestion des infrastructures critiques.

Contact : contact.ocd@orange.com

Tél : 01 47 08 88 00

orange™

PRENEZ DE LA HAUTEUR AVEC TREND MICRO POUR SÉCURISER VOTRE ENTREPRISE

Optez pour des solutions de sécurité simples, innovantes et sur mesure, pour protéger vos utilisateurs comme vos informations.

PROTECTION DES UTILISATEURS
Sécurisez vos postes de travail, serveurs et passerelles pour permettre l'accès aux données de votre entreprise en temps réel, depuis n'importe quel dispositif fixe et mobile.

PROTECTION DES ENVIRONNEMENTS VIRTUELS ET CLOUD
Profitez de solutions dédiées à la sécurisation des datacenters physiques, virtuels, Cloud ou hybrides.

PROTECTION CONTRE LES ATTAQUES CIBLEES
Détectez, neutralisez, analysez et gérez les attaques ciblées.

Plus d'informations sur www.trendmicro.fr

Créer un monde sécurisé

pour l'échange de données numériques

En tant que leader international de la sécurité, Trend Micro développe des solutions de sécurité innovantes qui rendent le monde plus sûr pour les entreprises et les particuliers échangeant des informations numériques. En tant que plus grande entreprise indépendante de sécurité au monde[1], avec plus de 25 ans d'expérience dans le domaine de la sécurité informatique, Trend Micro est reconnu comme leader sur le marché de la sécurité de serveur[2], de la sécurité de virtualisation[3] et de la sécurité de contenu pour petites entreprises[4]. Les solutions Trend Micro protègent les utilisateurs finaux, sécurisent les data centers d'aujourd'hui en constante évolution et bloquent les attaques ciblées sophistiquées. Trend Micro protège les données dans des environnements physiques, virtuels et Cloud et fournit une sécurité à la pointe de la technologie permettant de bloquer les nouvelles menaces plus rapidement.

1 Source : 2011 © Quocirca Ltd. : classement par chiffre d'affaires de fournisseurs indépendants de solutions de sécurité informatique
2 Source : 2012 IDC – Part des revenus mondiaux de la sécurité de points finaux pour entreprises, par fournisseur, pour 2011
3 Source : 2011 Technavio – Global Virtualization Security Management Solutions
4 Source : 2012 Canalys – Tendances du marché de sécurité de contenu pour petites entreprises, mars 2013

Les chiffres

- **Création :** 1988, États-Unis
- **Siège social :** Tokyo, Japon
- **Nombre d'employés :** 5 137
- **Cotation en bourse :** Bourse de Tokyo 4704
- **Chiffre d'affaires :** 1,2 milliard USD

Un passé riche en innovations : sécurisation du passage au Cloud

Depuis sa création, Trend Micro lance des technologies et services de sécurité innovants permettant de protéger les utilisateurs contre les menaces ciblant les plateformes émergentes et les nouveaux dispositifs. Trend Micro a été le premier à étendre la protection des ordinateurs de bureau aux serveurs, puis aux passerelles Internet.
La mobilité, la virtualisation et le Cloud Computing permettent de partager des informations numériques plus facilement, plus rapidement et à moindres frais. Dans ce contexte, Trend Micro continue d'innover dans la gestion de dispositifs mobiles, les technologies de réputation d'applications mobiles, le chiffrement des données, la détection de menaces avancées et la protection contre ces dernières, et l'optimisation de la sécurité pour les environnements Cloud et virtuels.

Garder une longueur d'avance

Souhaitant forger un monde plus sécurisé pour l'échange de données numériques et garder une longueur d'avance sur les cybercriminels, Trend Micro investit en continu dans la recherche sur les menaces afin de mettre au point des technologies, des produits et des services innovants. Trend Micro a pour objectif de bloquer les menaces plus rapidement et de fournir aux entreprises les renseignements utiles permettant de prendre des décisions éclairées sur la meilleure façon de protéger leurs données. Les clients sont ainsi certains de profiter des meilleures performances de protection, quelle que soit la plateforme utilisée.

Une protection intelligente, simple et adaptée

Trend Micro sécurise les dispositifs, les informations confidentielles et les données d'entreprise, permettant ainsi de profiter des avantages des nouvelles technologies tout en réduisant les risques au minimum.

L'offre Trend Micro propose en effet :

- une protection ***intelligente*** des informations, au moyen d'une sécurité intelligente en temps réel déployée à plusieurs niveaux sur les dispositifs mobiles, points finaux, serveurs et passerelles et dans le cloud ;
- des solutions ***simples*** mais flexibles au niveau de la gestion et du déploiement ;
- une sécurité ***adaptée*** à l'évolution de votre écosystème, optimisée pour s'intégrer en toute transparence aux technologies complémentaires, et améliorée en permanence pour relever les nouveaux défis de sécurité et faire face aux menaces les plus récentes.

La Stratégie 3C de Trend Micro

La stratégie 3C déployée par Trend Micro à l'intention de ses clients à travers le monde vise à maîtriser parfaitement les risques liés aux trois tendances que représentent le Cloud & la virtualisation, la consumérisation et les cyber-menaces évoluées. Cette sécurité se décline donc en trois volets :

- **Complete User Protection** : la protection intégrale des utilisateurs sur site et nomades dans leurs activités au quotidien
- **Cloud and Data Center Security** : la sécurité dédiée aux environnements Cloud et virtualisés
- **Custom Defense** : la maîtrise des cyber-attaques ciblées et des menaces évoluées

Chacun de ces volets associe des technologies et des services pertinents pour concrétiser une sécurité capable de défendre les entreprises et d'en assurer la pérennité.

Des renseignements sur les menaces à l'échelle mondiale

S'appuyant sur des méthodes d'analyse de données de masse pour traiter en continu plus de 4 téraoctets de données collectées au niveau du Cloud, l'infrastructure **Trend Micro™ Smart Protection Network™** (SPN) permet d'identifier les menaces, d'offrir une protection proactive et de sécuriser efficacement les données. SPN bloque plus de 230 millions de menaces par jour.

Par ailleurs, grâce aux **TrendLabs℠**, son réseau mondial de recherche sur les menaces, de service produits et d'assistance, Trend Micro protège à toute heure des dizaines de millions de clients. 1 200 experts surveillent ainsi les menaces potentielles et offrent des solutions rapides aux principaux incidents de sécurité et aux demandes d'assistance urgentes. Au fur et à mesure qu'émergent de nouvelles menaces et que se forment de nouvelles vulnérabilités, les TrendLabs permettent l'accès à une sécurité globale au moyen de renseignements personnalisés dont les clients ont besoin pour protéger leurs activités en ligne.

Le numérique au cœur
de la deuxième édition du Concours Mondial d'Innovation

Le 18 avril 2013, le Président de la République a mis en place la **Commission «Innovation 2030»**, présidée par Anne LAUVERGEON, sous l'égide du Ministre du Redressement productif et de la Ministre déléguée chargée des Petites et Moyennes Entreprises, de l'Innovation et de l'Économie numérique. Cette Commission s'est appropriée les principaux enjeux du monde de 2030 et a identifié un nombre limité d'opportunités majeures au potentiel particulièrement fort pour l'économie française.

A l'issue de ces travaux, 7 premières ambitions ont vu le jour.

C'est dans cette perspective que l'Etat a initié la première édition Concours Mondial d'Innovation. Fort de son succès, une deuxième édition s'organisera autour d'une nouvelle ambition : « **sécurité collective et protection contre les actions malveillantes** ». En effet, les solutions innovantes de sécurité contribuent de façon majeure à la sécurité collective, et des personnes, à la résilience de la Nation et à la compétitivité de notre industrie. Cette deuxième édition permettra ainsi de soutenir les projets les plus innovants dans ce domaine. Le secteur de la sécurité numérique, des grands groupes aux très petites entreprises (TPE), est particulièrement concerné par cette nouvelle ambition.

L'objectif de ce concours est de faire **émerger les talents et futurs champions de l'économie française** en les repérant puis en accompagnant la croissance des entrepreneurs français ou étrangers dont le projet d'innovation présente un potentiel particulièrement fort pour l'économie française.

Le Gouvernement souhaite ainsi attirer les talents du monde entier pour qu'ils réalisent leurs projets en France. Dans le cadre du Programme d'Investissements d'Avenir et en s'appuyant sur Bpifrance (la banque publique d'investissement), l'Etat affectera un montant de plus de **300 millions d'euros pour co-financer les projets les plus innovants répartis sur les 8 ambitions fixées par la Commission.**

CYBERCERCLE

Le club de réflexion sur la sécurité numérique
sous dynamique parlementaire

Rejoignez le CyberCercle

Un cadre privilégié d'accès à l'expertise, d'échanges et de rencontres sur les questions de sécurité numérique

Petits déjeuners débats
Des matinales thématiques
en présence d'experts et de parlementaires

Rencontres Parlementaires de la Cybersécurité
Le rendez-vous institutionnel annuel de la communauté française de la cybersécurité et du numérique

Rencontres Régionales de la Cybersécurité
Des journées d'information
ancrées dans une dynamique locale

Cybersécurité & Parlement
La lettre d'information parlementaire
qui donne la parole aux spécialistes

Rencontres Parlementaires
Cybersécurité & milieu maritime
Une demie-journée d'échanges réunissant les institutionnels français de la cybersécurité et du milieu maritime

CyberCercle Formation
L'offre de formation en droit, management, organisation et gestion de crise sur la cybersécurité

Merci à nos partenaires

Partenaires médias

09 83 04 05 37
contact@cybercercle.com
@CyberCercle