Forum International de la cybersécurité

Lille 22/23 janvier 2019

DOSSIER DE PRESSE

Forum International de la Cybersecurité

SECURITY AND PRIVACY BY DESIGN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

SOMMAIRE

Edito

Chaque jour, la cybersécurité est plus nécessaire pour notre pays.

Nos quotidiens sont connectés, ils sont aussi épiés, espionnés. Nos systèmes d'information décuplent nos capacités, font vivre nos économies; ils sont attaqués, parfois pillés. Nos opérations, aussi, notre défense et notre sécurité reposent plus que jamais sur les progrès et les opportunités du numérique. Ne soyons pas naïfs, il peut aussi les menacer. L'année dernière au Forum international de la cybersécurité, je faisais une promesse : celle d'Armées à la pointe de la cybersécurité.

Un an plus tard, je suis fière de revenir à Lille avec des promesses tenues. La loi de programmation militaire 2019-2025 a été votée, elle prend le tournant du numérique et avec 1,6 milliard d'euros et 1 000 cyber-combattants supplémentaires, elle consacre des moyens exceptionnels à la lutte dans l'espace numérique.

Le ministère des Armées s'est également doté des structures essentielles pour réussir le défi de la cybersécurité. La direction générale du numérique a été créée, elle est le chef d'orchestre de la révolution numérique du ministère. L'agence pour l'innovation de défense rassemble tous les entrepreneurs, chercheurs, innovateurs qui veulent trouver des solutions nouvelles, notamment pour notre sécurité cyber. Le commandement de la cyberdéfense est renforcé. J'ai, enfin, la semaine dernière, annoncé des doctrines claires, défensives et offensives, pour notre cyberdéfense. Alors, face au défi de la cybersécurité, le ministère des Armées prend résolument ses responsabilités. Mais cet effort doit être collectif.

Nous devons aussi nous tourner vers nos partenaires et nos alliés. Les menaces cyber pèsent sur tous les pays d'Europe et nous avons tout intérêt à unir nos efforts plutôt qu'à combattre les attaques en ordre dispersé. L'union fait la cyberdéfense et je n'imagine pas l'Europe de la défense sans son volet cyber.

Mais ce n'est pas tout : chaque entreprise, chaque partenaire du monde de la défense a son rôle à jouer. Nos adversaires chercheront tous les moyens pour nous atteindre, cela implique bien sûr les industriels, leurs sous-traitants et même certains particuliers. Le ministère des Armées et les entreprises doivent travailler ensemble, se coordonner. Les bonnes pratiques et les méthodes partagées peuvent éviter des failles béantes. L'« hygiène cyber » n'est donc pas un luxe, c'est une absolue nécessité. Le thème du FIC 2019 ne pouvait donc pas mieux tomber. Security and privacy by design : c'est en effet par essence que nous devons penser la cybersécurité et l'intégrer dans nos systèmes à chaque étape. En nous forçant à prendre en compte dès le départ la cybersécurité, nous renforçons notre protection, celle de nos données. Nous limitons les risques et nous envoyons un message fort : nous sommes prêts.

La 11e édition du FIC sera une nouvelle fois l'occasion d'échanges et de débats passionnants. Je remercie tous ceux, acteurs publics et privés, français et internationaux, qui, une nouvelle fois, prennent part à ce forum.

Je souhaite au FIC 2019 un plein et brillant succès !

Florence Parly
Ministre des Armées

Le ministère des Armées au Forum international de la cybersécurité

Le ministère des Armées participe les 22 et 23 janvier 2019 à la onzième édition du Forum international de la cybersécurité (FIC) qui se tiendra à Lille-Grand Palais.

La thématique de cette nouvelle édition : Security and privacy by design.

Partenaire historique, le ministère s'associe chaque année à ce rendez-vous incontournable pour la communauté numérique française et européenne.

Différentes entités du ministère seront présentes, à travers un stand de 90m² mettant en avant l'innovation au cœur de la cybersécurité, des présentations dynamiques grâce à un espace dédié et les plénières et ateliers du salon.

Ainsi, cet événement sera l'occasion pour le Commandement de la cyberdéfense (COMCYBER), la Direction générale de l'armement (DGA), la Direction du renseignement et de la sécurité de la Défense (DRSD), la Direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI), les réserves de cyberdéfense et les armées de présenter leurs missions, leurs spécificités et leurs capacités.

Une nouvelle structure du ministère des Armées accompagnera cette année les experts de la cybersécurité : l'Agence de l'innovation de Défense (AID).

Les objectifs du ministère à travers cette participation sont de témoigner auprès du grand public de son expertise et d'assurer la promotion des métiers du numérique au sein des différentes entités.

À cet effet, la Marine nationale tiendra également un stand sur le nouvel espace du FIC dédié au recrutement.

À noter également au programme de cette année, une table-ronde dédiée aux cyber-commandeurs.

Suivez l'actualité du ministère des Armées sur le salon.

Durant toute la durée du salon, retrouvez toutes les informations et l'actualité du ministère des Armées (brèves, vidéos, photographies et webtv) sur le site Internet defense.gouv.fr et sur les réseaux sociaux : Twitter (@Defense_gouv #FIC2019) et Facebook (Defense.gouv), également sur les comptes Twitter du COMCYBER @ComcyberFR et de l'Agence de l'innovation de Défense @Agence_

Les entités présentes sur le stand du ministère des Armées

COMCYBER

Le COMCYBER, sous l'autorité directe du chef d'état-major des armées, est responsable de la manœuvre cyber globale des armées.

Créé en 2017, le COMCYBER a pour mission :

- la protection des systèmes d'information de l'état-major des armées ;
- la conduite de la défense des systèmes d'information du ministère des Armées (hors DGSE et DRSD) ;
- la conception, la planification, la conduite des opérations militaires dans l'espace numérique ;
- la contribution à la préparation de l'avenir du domaine de la cyberdéfense.

Doté d'un état-major opérationnel, le COMCYBER s'appuie sur les unités spécialisées en cyberdéfense des armées et organismes interarmées qui constituent un vivier de 3 400 cyber-combattants au sein du ministère, ainsi que sur la Réserve cyber.

FOCUS : RÉSERVE CYBER

Créé en septembre 2015, le Centre de la réserve et de la préparation opérationnelle de cyberdéfense (CRPOC) est l'acteur majeur du recrutement des réservistes de cyberdéfense et de la préparation opérationnelle des forces. Le CRPOC, en lien avec le COMCYBER et les armées, a notamment à sa charge l'organisation de l'exercice annuel interarmées DEFNET.

LE CENTRE DE LA RÉSERVE ET DE LA PRÉPARATION OPÉRATIONNELLE DE CYBERDÉFENSE (CRPOC) ASSURERA UNE PERMANENCE SUR LE STAND FIC.

Direction générale de l'armement (DGA)

La DGA est l'expert technique référent du ministère en matière de cybersécurité. De l'anticipation de la menace à la mise en œuvre de cybersolutions pour les armées et les hautes autorités de l'État, elle assure, depuis la conception d'algorithmes cryptographiques jusqu'aux architectures sécurisées de systèmes complets :

- un rôle de conseil et de soutien à la lutte informatique défensive du ministère des Armées ;
- le développement et l'évaluation de produits de cybersécurité ;
- la prise en compte de la cybersécurité dans tous les programmes d'armement ;
- l'animation de la R&T (recherche et technologie) cyber en lien avec les autres entités étatiques, l'industrie et le monde de la recherche.

La DGA renforcera son expertise technique déterminante pour la souveraineté de la France par le recrutement de spécialistes de haut niveau (plus de 600 experts fin 2019 pour atteindre 900 en 2025).

DGA Maîtrise de l'information, établi à Bruz (35) est le centre d'expertise et d'essais de la DGA de référence pour la cybersécurité.

Retrouvez plus d'informations à l'adresse suivante :

https://www.defense.gouv.fr/dga

FOCUS : DGA MAITRISE DE L'INFORMATION

DGA Maîtrise de l'information est l'expert technique du ministère des Armées pour les systèmes d'information et de communication, la cybersécurité, la guerre électronique et les systèmes de missiles tactiques et stratégiques. Son expertise s'exerce du composant électronique aux systèmes de systèmes, pour tout type de milieu (terrestre, naval, aérien, spatial, cyber). Pour répondre aux enjeux de défense d'aujourd'hui et de demain, et toujours garder l'avance nécessaire à la protection de notre nation, le centre de DGA Maîtrise de l'information se développe rapidement dans tous les domaines technologiques actuels, tels que la cybersécurité, l'intelligence artificielle et le traitement massif des données. Il participe activement à l'animation de la filière stratégique cyber, tant sur le plan de la formation et de la recherche que sur celui du développement des entreprises françaises innovantes, en particulier au sein du Pôle d'excellence cyber.

Direction générale du numérique (DGNUM)

Prenant la mesure de la révolution numérique, le ministère des Armées a créé la Direction générale du numérique et des systèmes d'information et de communication (DGNUM) en juin 2018.

Remplaçant la Direction générale des systèmes d'information et de communication (DGSIC) créée en 2006 et directement rattachée à la ministre, la DGNUM est dotée de pouvoirs élargis lui permettant d'assurer la cohérence globale des systèmes d'information et de communication du ministère des Armées et d'améliorer les conditions dans lesquelles sont conduits les projets. Cela passe notamment par davantage d'agilité dans les processus.

Cet objectif se traduit au travers de deux missions principales :

- Orchestrer la transformation numérique au profit des armées, directions et services en tirant parti des ruptures technologiques et en plaçant l'usager au cœur de la démarche ;
- assurer une gouvernance renforcée de la fonction SIC en lien étroit avec les trois grands subordonnés du ministre (EMA, DGA, SGA) et le cabinet de la ministre.

La donnée étant au cœur de la transformation numérique, le DGNUM assume la fonction d'administrateur ministériel des données. A l'instar de l'administrateur général des données pour le niveau interministériel, il a pour mission de coordonner l'action des armées, directions et services en matière d'inventaire, de gouvernance, de production, de circulation, de partage et d'exploitation des données au sein du ministère des Armées ainsi que de favoriser l'accessibilité des données entre administrations ou dans le domaine public, dans un format ouvert et réutilisable.

FOCUS : PRIX DSI ORCHESTRATEUR 2019

Le VAE Coustillière, lauréat du prix « DSI Orchestrateur 2019 », décerné par le magazine IT for Business.

Démarche volontariste visant à s'approprier au plus vite et dans les meilleures conditions les technologiques émergentes, le projet « Défense Connect » de transformation numérique du ministère des Armées a été mis à l'honneur mercredi 16 janvier 2019 par les professionnels du secteur du numérique. Le VAE Arnaud Coustillière a ainsi reçu le prestigieux prix de « DSI Orchestrateur », soulignant le chemin parcouru par le projet Défense Connect qui fête fin janvier sa première année d'existence. C'est également le premier militaire tous prix confondus, à être distingué depuis leur création en 1999.

Au-delà de la DGNUM, ce prix récompense de manière collective le travail réalisé par tous les métiers du ministère. Armées, Directions, Services, notamment par le biais de leurs Directeurs de la Transformation Digitale (DTD), sont au cœur de ces travaux et des réalisations concrètes que chacun voit émerger au quotidien. Enfin, ce prix illustre l'importance du projet Défense Connect dans la modernisation et l'attractivité du ministère, tant au niveau interministériel qu'en direction de notre écosystème partenaire.

Direction du renseignement et de la sécurité de la Défense (DRSD)

Service de renseignement du ministère des Armées, la DRSD a pour mission de « renseigner pour protéger » les forces armées et les entreprises de Défense.

Dans le domaine cyber, la DRSD anticipe et accompagne la révolution numérique. Elle identifie les vulnérabilités et les menaces susceptibles de porter atteinte aux personnes, matériels et informations sensibles du ministère.

S'appuyant sur ses moyens propres, la DRSD travaille avec de nombreux partenaires. Elle participe ainsi à la lutte informatique en protégeant les systèmes d'information du ministère et des entreprises de défense.

Retrouvez plus d'informations à l'adresse suivante : www.defense.gouv.fr/drsd

Agence de l'innovation de défense (AID)

Placée sous la responsabilité du Délégué général pour l'armement (DGA), l'Agence de l'innovation de défense a été créée le 1er septembre 2018 par Florence Parly, ministre des Armées. Cette nouvelle organisation, dirigée par Emmanuel Chiva, doit inventer de nouveaux modes d'intervention du ministère, de nouveaux outils, notamment pour favoriser les expérimentations rapides. Résolument tournée vers l'innovation civile, l'agence doit nouer des partenariats avec les écosystèmes les plus innovants, dans les domaines académique, entrepreneurial, mais aussi intraprenarial car les sources de l'innovation sont autant internes qu'externes. Elle oriente l'ensemble des études du ministère, avec un budget qui atteindra plus d'un milliard et demi d'euros en 2022, tel que prévu dans la prochaine Loi de programmation militaire. Cette nouvelle agence implique toutes les composantes du ministère, et notamment les armées, dans sa gouvernance. Elle est résolument tournée vers l'Europe et tire pleinement parti de l'opportunité formidable qu'est aujourd'hui le fonds européen de défense.

Retrouvez plus d'informations sur Twitter : @Agence_ID

Direction interarmées des réseaux d'infrastructure et des systèmes d'informations de la défense (DIRISI)

Opérateur ministériel des SIC, la DIRISI conçoit, développe, sécurise et défend les moyens qu'elle met en œuvre. Elle gère les architectures des systèmes d'information et de communication, des opérations extérieures (réseaux informatiques, moyens radios et satellitaires) aux datacenter et structures d'hébergement modernes ainsi que les différents réseaux du ministère. Acteur de la transformation digitale, elle déploie le socle technique des engagements opérationnels de demain.

La DIRISI recrute dans tous les métiers de l'informatique, alors pourquoi pas vous ?

Découvrez plus d'informations en scannant le QR code :
Et à l'adresse suivante :
https://www.linkedin.com/company/dirisi/

Armée de terre : Commandement des systèmes d'information et de communication (COMSIC) des forces terrestres

Au sein du COMSIC, l'école des Transmissions est le pôle de compétence et d'expertise de l'armée de Terre pour la formation du personnel militaire et civil servant dans les domaines des Systèmes d'information et de communication (SIC), de la Guerre électronique (GE) et de la cybersécurité. Dans ce domaine, l'école des Transmissions conçoit et réalise une trentaine de formations depuis le niveau Bac jusqu'au niveau Bac +6. Positionnée au sein d'un écosystème cyber régional particulièrement riche, elle accueille plus de 900 stagiaires en cybersécurité par an, civils et militaires des trois armées et est ouverte à l'international. En lien permanent avec, non seulement, les armées et les forces terrestres mais, également, le Pôle d'excellence cyber (PEC), le COMSIC contribue activement aux processus d'innovation du ministère des Armées.

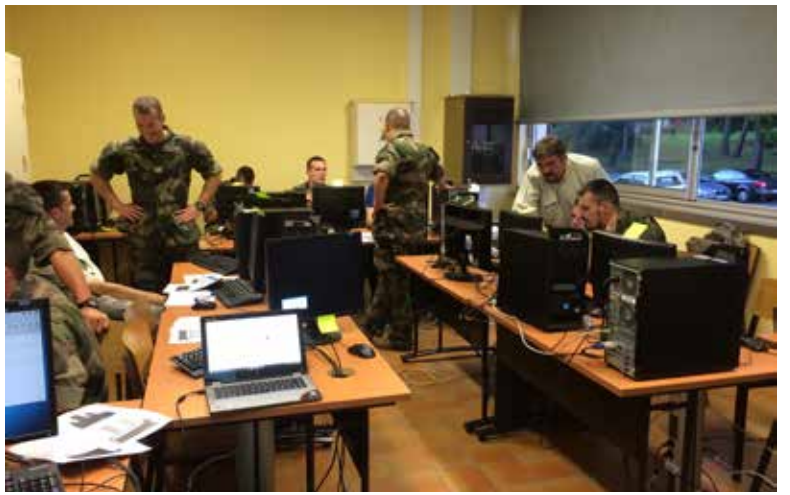
Retrouvez plus d'informations à l'adresse suivante :
http://www.esat.terre.defense.gouv.fr

Armée de terre : Mastère Spécialisé en cyberdéfense

Le Mastère Spécialisé en Cyberdéfense répond au besoin de former des officiers et cadres généralistes des opérations dans l'espace numérique, employés dans des fonctions d'officiers de sécurité des systèmes d'information de grande unité ou de zone, d'officiers de lutte informatique défensive, en cellule cyber d'État-major ou dans les forces projetées, et qui rejoindront la filière cyber après un cursus éventuellement hors sécurité des systèmes d'information. Ces officiers doivent disposer d'un socle technique mis à jour, de compétences en gestion de crise, ainsi que dans différents domaines des sciences sociales et politiques. Ils doivent maîtriser certaines compétences professionnelles fondamentales : évaluation de la menace, planification des opérations, gestion des projets, anticipation des risques cyber... La formation est accréditée par la Conférence des grandes écoles ; elle est délivrée en partenariat par les écoles de Saint-Cyr Coëtquidan et l'école de transmission (ETRS) de Rennes. Intégrant la semaine de formation des officiers cyber de haut niveau, elle donne lieu à la délivrance d'un Diplôme Technique et du titre de Mastère Spécialisé (BAC+6). La formation comporte une partie académique (environ 450 heures), une mission professionnelle (4 mois) et la préparation d'une thèse professionnelle. Elle peut être menée en une année pleine (sept mois de formation académique avant la mission professionnelle et la rédaction de la thèse) ou sur deux années (à raison de trois jours

par mois. La formation peut être ouverte à des officiers étrangers francophones et à des cadres de l'administration publique ou des opérateurs d'importance vitale.

Découvrez un reportage sur
« Les combattants numériques » en scannant le QR code :



Marine nationale

La Marine nationale a créé le Centre de support cyberdéfense (CSC) pour faire face aux menaces cyber, évaluées par le Livre Blanc comme « de première importance ». Le CSC contribue à la chaîne opérationnelle de cyberdéfense. Il a pour rôle de garantir que les équipages des unités opérationnelles et des centres de commandement de la Marine ont acquis les réflexes indispensables pour faire face à tout événement de cyber sécurité se produisant sur leurs systèmes numériques.

C'est la raison pour laquelle la Marine recrute plus de 35 profils officiers cyber en 2019.

Le service de recrutement de la Marine sera présent sur le nouvel espace dédié du FIC.

Retrouvez plus d'informations à l'adresse suivante : https://www.etremarin.fr/

Armée de l'Air

L'armée de l'Air assure la cyberdéfense des réseaux informatiques et des systèmes de combat qu'elle opère. Elle s'appuie sur l'engagement d'aviatrices et d'aviateurs spécialistes du domaine, en métropole comme en opérations extérieures. Ce vivier d'experts assure au quotidien le maintien des meilleurs standards de sécurité informatique, et arme le dispositif de veille et d'alerte opérationnel de cyberdéfense de l'armée de l'Air.

Connectée à la société civile, l'armée de l'Air soutient également l'écosystème de cybersécurité régional en s'engageant en faveur de la jeunesse et d'entreprises du numérique innovantes.

Temps forts pour le ministère des Armées

Les ateliers et plénières

Mardi 22 janvier :

11h : Ouverture du *policy challenge* par le général de division Olivier Bonnet de Paillerets, commandant de la cyberdéfense

12h – 13h15 : Atelier « *Technologies de Défense Active* »

En présence de M. Sébastien Bombal, Conseiller du COMCYBER

17h – 19h : Plénière « *L'autonomie stratégique à l'épreuve du numérique* »

En présence du vice-amiral d'escadre Arnaud Coustillière, Directeur général du numérique et des systèmes d'information et de communication

17h15 : Discours de la ministre en plénière

Mercredi 23 janvier :

9h – 11h : Plénière « *Cyberattaques : Peut-on inverser le rapport de force ?* »

En présence du général de division Olivier Bonnet de Paillerets, commandant de la cyberdéfense

13h30 – 14h15 : Table-ronde : « *Analyses nationales de la cybermenace, réponses nationales et réponses dans le cadre de coalitions ou de partenariats* »

En présence du Général de division Olivier Bonnet de Pailleret, commandant de la cyberdéfense et de ses homologues (Estonie, Allemagne, Japon et Suisse). Modérateur : Général d'Armée aérienne (2s) Jean-Paul Paloméros

15h – 16h : Atelier : « Innover en cyber sécurité, oui mais comment ? »
En présence de M. Bertrand Blond Conseiller capacitaire du COMCYBER

Atelier « Cybersécurité : comment choisir son prestataire de cloud public ? »

Démonstration d'un projet soutenu par l'Agence de l'innovation de Défense : Le logiciel LINTY

Linty analyse le code informatique VHDL fréquemment utilisé pour programmer des fonctions cryptographiques ou des composants sécuritaires.

Il détecte automatiquement les erreurs de programmation (bugs et vulnérabilités) qui pourraient conduire à des défaillances.

Ce logiciel innovant permet de réduire les risques de développement en détectant très tôt de nombreuses anomalies.

DGA - Défi Cyber

Porté par la DGA en relation avec l'AID, le Défi cyber lancé en septembre 2018 vise à faire émerger une solution innovante, expérimentable par les forces armées, pour l'investigation à distance à des fins de défense, des cyberattaques sur les réseaux du ministère des Armées. Les deux lauréats du Défi cyber seront présents sur le stand du ministère pour présenter leurs solutions, et l'un d'entre eux sera déclaré vainqueur du challenge. Il verra son prototype testé au sein du ministère des Armées.

FOCUS : LE DÉFI CYBER DE LA DGA

Dans un marché dominé par de grands acteurs internationaux, la Direction générale de l'armement (DGA) veut favoriser l'émergence d'une solution innovante portée par une startup ou une PME/ETI française, permettant de mener des investigations à distance sur des cyberattaques visant les réseaux informatiques du ministère des Armées.

L'objectif est de prototyper des solutions présentant des fonctionnalités pour effectuer plus rapidement certaines opérations de prélèvement ou d'analyse sur différents équipements des réseaux, de manière automatisée et à distance, en prenant en compte les différentes contraintes liées aux réseaux du ministère des Armées.

Les deux lauréats retenus seront présents sur le stand de la DGA pour présenter les démonstrateurs qu'ils ont conçus :

Hurukai, proposée par les sociétés Harfanglab et Gatewatcher, est une solution d'investigation numérique adaptée aux contraintes opérationnelles des armées pour accélérer la détection des attaques, investiguer sans impact sur les métiers, et détruire la menace avec précision. Cet agent logiciel léger et intelligent permet de rechercher des compromissions sur des parcs informatiques, propose une boîte à outils pour la réponse à des incidents et remplit la fonction d'agent d'alerte pour les réseaux sensibles.

Myrmex, de la société Amossys, permet une recherche pointue, rapide et discrète de compromission système. Composé d'une suite de cinq outils complémentaires, il permet de mener des opérations de prélèvement ou d'analyse sur des équipements réseaux, de manière automatisée et à distance, ainsi qu'un travail collaboratif entre analystes.

La solution du vainqueur du Défi cyber de l'édition 2019 du FIC sera testée au sein du ministère des Armées.

FIC Challenge

Pour la 5e année consécutive, avec le parrainage du COMCYBER et en partenariat avec la Gendarmerie nationale, le Conseil régional des Hauts-de-France et CEIS (Compagnie européenne d'intelligence stratégique), l'École pour l'informatique et les techniques avancées (EPITA) et ACISSI (Audit, Conseil, Installation et Sécurisation des Systèmes d'Information) organisent deux challenges. Ces deux challenges sont développés et animés respectivement par les étudiants de l'EPITA et l'association ACISSI. D'une durée de 4h, ils distinguent des profils prometteurs, encouragent et valorisent les métiers liés à l'investigation numérique et à la lutte informatique défensive.

Informations pratiques

ACCÈS

Lille Grand palais

1 boulevard des Cités Unies

59777 Lille - Euralille

HORAIRES DU SALON

Mardi 22 janvier 2019 de 9h00 à 19h00

Mercredi 23 janvier 2019 de 9h00 à 18h00

Retrouvez plus d'informations sur le site du FIC :

https://www.forum-fic.com/

DICoD

Centre de presse
Officier de presse du ministère des Armées
Tél : 09 88 67 33 33
presse@dicod.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

Ministère des Armées

@Defense_gouv

@ministeredesarmees

Retrouvez-nous sur www.defense.gouv.fr