Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

DOSSIER D'INFORMATION

24 septembre 2015
Paris – École militaire

Contact :
Centre de presse,
Délégation à l'information et à la communication de la Défense
Tél : 01.44.42.54.02
Mail : presse@dicod.defense.gouv.fr

DICoD

@Defense_Gouv / #CyberDefense

Sommaire

Edito de Jean-Yves Le Drian, ministre de la Défense

Je suis heureux de vous accueillir au colloque #CyberDefense : le combat numérique au cœur des opérations, premier événement de la cyberdéfense militaire.

Engagée dans des opérations militaires sur plusieurs théâtres, seule ou en coalition, la France a pris l'initiative de rassembler aujourd'hui, autour des autorités et des experts du ministère, les grands partenaires de la cyberdéfense militaire, des pays du Maghreb et des pays du Golfe, des représentants de l'OTAN et de l'UE. Nos forces armées sont en effet confrontées en permanence à des menaces cybernétiques susceptibles de compromettre l'autonomie de décision, la sécurité et le succès de nos opérations.

La coopération internationale est indispensable dans ce domaine militaire qui ne connaît pas de frontières. Ce séminaire #CyberDefense, au travers de thématiques reflétant les préoccupations actuelles de la communauté militaire de cyberdéfense, CyberDefense vise à promouvoir et renforcer cette coopération, du partage d'informations à l'interopérabilité de nos capacités. Les experts de plusieurs pays animeront ces travaux.

Cet événement permettra aussi de mener une compétition « cyberdéfense » amicale entre les académies militaires françaises, américaines et estoniennes, et d'organiser un challenge au profit des candidats réservistes en lien avec différentes écoles et facultés.

Je vous souhaite à tous un excellent séminaire riche d'échanges et de partage d'expériences autour d'une thématique qui vous rassemble aujourd'hui : le combat numérique au cœur des opérations militaires. »

Présentation #CyberDefense

Le 24 septembre, le ministère de la Défense organise «#Cyberdefense 2015 », le premier colloque international consacré à la cyberdéfense. Réalisé en partenariat avec le soutien des industriels français du secteur, ce colloque sera inauguré par le ministre de la Défense, Jean-Yves Le Drian et son homologue britannique Michael Fallon.

Priorité nationale, la cyberdéfense constitue désormais un cinquième champ de bataille pour la défense des intérêts français. Pour cette première édition, le thème abordé est « la cyberdéfense au cœur des opérations ». Il vise à illustrer l'investissement du ministère de la Défense dans cette lutte d'un nouveau genre et à mieux en cerner les implications et les enjeux dans le cadre des opérations militaires.

#Cyberdefense rassemble les hauts responsables de la cyberdéfense française et mondiale, issus d'une vingtaine de pays alliés. Des responsables de la Défense, des étudiants et experts universitaires, des entreprises ou encore des représentants d'organisations internationales, seront présents pour croiser les expériences et approfondir les connaissances de chacun.

Pour cette première édition, la DGA et l'EMA Cyber lancent deux challenges destinés aux étudiants d'écoles d'ingénieurs civils et militaires situées en France et à l'étranger. Il s'agit d'évaluer le niveau de connaissance des futurs ingénieurs et à tester leurs aptitudes dans des exercices de simulation d'attaques informatiques grandeur nature. Pour les étudiants et la communauté Défense, ces challenges permettent aussi de commencer à fédérer un réseau international de futurs experts en cyberdéfense.

- **Suivez l'actualité du ministère de la Défense sur le colloque**

Durant le colloque, retrouvez toutes les informations et l'actualité du minsitère de la Défense (brèves, vidéos, photographies et web-tv) sur le site internet www.defense.gouv.fr . Suivez l'ensemble de la journée sur les réseaux sociaux :

- Twitter : @Defense_Gouv - #Cyberdefense
- Facebook.com/defense.gouv

La cyberdéfense : une priorité nationale

La cyber-guerre, c'est la guerre de demain, elle commence déjà aujourd'hui, et la Loi de programmation militaire que j'ai présentée au Parlement intègre cette nouvelle donnée. Demain, il y aura une quatrième armée qui s'appellera l'armée cyber, demain il y aura des soldats cyber. Nous avons les moyens de réagir, nous avons aussi les moyens d'attaquer, mais nous sommes en situation de pouvoir répondre, parce que la cyber-guerre c'est vraiment un outil majeur, contre lequel il faut se défendre, et la France est au rendez-vous.

Jean-Yves Le Drian, ministre de la Défense, Europe 1, le 13 janvier 2015

- **La cyberdéfense au sein du ministère de la Défense**

La cyberdéfense militaire regroupe l'ensemble des actions défensives ou offensives conduites dans le cyberespace. Elle vise à 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 cyberdéfense militaire regroupe l'ensemble des actions défensives ou offensives conduites dans le cyberespace pour 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.

- **Le renforcement des moyens mis en œuvre pour la cyberdéfense**

L'actualisation de la Loi de programmation militaire (LPM) a renforcé significativement les moyens dévolus à la cyberdéfense. En complément des projets spécifiques mis en place et de l'augmentation des investissements humains et financiers, l'effort consacré à la cyberdéfense se traduit également par une série de mesures connexes, telles que des exercices d'entraînement des forces cyber ou des journées de sensibilisation à la cybersécurité au sein de chaque unité militaire.

- **Le Pacte Défense Cyber**

Le ministre de la Défense, Jean-Yves Le Drian, a lancé le « Pacte Défense Cyber » le 7 février 2014. Comptant parmi les priorités de la Loi de programmation militaire (2014-2019) votée en avril 2013, il est prévu de doter ce pacte d'un milliard d'euros. Témoignant d'une ambition politique forte, ce plan vise à protéger la souveraineté de la France sur le long terme, et en faire une nation qui compte dans le cyberespace mondial.

Le programme de la journée

9 h 30
(Amphi Foch)

Discours d'ouverture par le ministre de la Défense et son homologue britannique

10 h 00
(Amphi Foch)

Conférence : l'évolution des menaces dans l'espace numérique

L'espace numérique est un nouvel espace de confrontation et les événements en témoignent. Sous la conduite de la titulaire de la Chaire Castex, Frédérick Douzet, des experts civils et des militaires de haut niveau, français et américains, échangeront leurs visions sur l'évolution des cybermenaces.

11 h 30

Ateliers thématiques

(Amphi Sabatier)

- **Retour d'expérience des exercices nationaux et interalliés**

Le commandement des États-Unis en Europe (EUCOM) organise annuellement le plus grand exercice d'interopérabilité, *Combined endeavour*, associant notamment les membres de l'OTAN. Celui-ci comporte un volet cyberdéfense. *DefNet* est l'exercice de cyberdéfense des armées françaises. L'édition 2015 a été l'occasion d'expérimenter le concept de réserve opérationnelle de cyberdéfense à vocation nationale.

(Amphi De Bourcet)

- **Organisation du commandement et de la doctrine en coalition : l'interopérabilité**

En raison de menaces cyber de plus en plus transverses, l'existence d'une coalition interalliées s'avère indispensable. Cependant, les capacités souveraines nationales, par essence confidentielles, freinent bien souvent l'interopérabilité entre systèmes.

(Salle SS 1
Amphi Foch)

- **Les *advanced persistent threats* (APT) en milieu militaire**

Les APT sont particulièrement nuisibles car elles ciblent de manière furtive et invisible une entité spécifique. Sur les systèmes d'information militaires, elles peuvent avoir des conséquences graves sur le déroulement des opérations.

- **Présentation de solutions par des PME**
- **Exercice de planification sur table (sur invitation)**

En parallèle, réunion d'échange au format « cyber commandeurs »

12 h 30

Déjeuner et découverte des stands pour les visiteurs au pavillon Joffre
Déjeuner avec le ministre à la Rotonde pour les VIP

14 h 30

Remise des trophées

14 h 45 **Ateliers thématiques**

(Amphi Sabatier) **Capacités de formation et d'entraînement à la gestion de crise**

La formation et l'entraînement constituent les deux éléments clés permettant une gestion de crise efficace.

(Salle SS 1 Amphi Foch) **La cyberdéfense et la propagande de *Daesh* : menaces et réponses**

Daesh a su s'adapter aux moyens de communication modernes et à leurs évolutions constantes. L'espace numérique constitue désormais l'un de ses vecteurs principaux de communication et de propagande. *Daesh* l'utilise à des fins de recrutement en adaptant son message suivant les nations ciblées. Pour s'en protéger, les États doivent mettre en place des moyens de lutte efficaces mais surtout cohérents.

(Amphi De Bourcet)

- **Création d'une plateforme nationale d'échanges sur les menaces informatiques entre les industriels de l'armement et le ministère de la Défense (sur invitation)**
- **Poursuite de la présentation de solutions par des PME**
- **Poursuite de l'exercice sur table (sur invitation)**

En parallèle, rencontres bilatérales entre les cyber commandeurs

16 h 30 (Amphi Foch) **Conférence conjointe des cyber commandeurs : la cyberdéfense au cœur des opérations par la mise en œuvre des capacités offensives et défensives dans le cadre d'une coalition.**

La cyberdéfense est désormais considérée comme un enjeu majeur de la conduite des opérations. Sous la conduite du vice-amiral Coustillière, les cyber commandeurs présents partageront leurs expériences et exposeront les différentes étapes nécessaires à la mise en place de capacités de cyberdéfense dans le cadre d'opérations militaires menées en coalition.

17 h 30 (Amphi Foch) **Discours de clôture par le sous-chef opérations de l'état-major des armées**

<u>A l'occasion du colloque :</u>

- Présentation de stands par les entreprises partenaires autour de l'amphithéâtre Foch ;
- Challenge des grandes écoles militaires (3 françaises, 1 américaine, 1 estonienne) du 23 soir au 24 fin de matinée ;
- Défi #Cyberdefense des écoles civiles d'ingénieur le 24 matin.

<u>Éléments particuliers concernant le ministre :</u>

- Micro-tendu dans le hall de l'amphi Foch

- Visite des stands de 10h15 à 10h45.

Les challenges des écoles

Challenge #CyberDefense

6 écoles militaires internationales s'affrontent lors de cette compétition amicale : l'école navale française, l'école de l'air française, Saint-Cyr Cöetquidan, la ligue de défense cyber estonienne, l'*United States Naval Academy,* l'*United States Military Academy.*

À partir du 23 septembre à 20h00 et jusqu'au 24 septembre à 12h00, chaque école, composée d'une équipe de 10 personnes, doit protéger le système de gestion informatique d'un ensemble industriel – ici, des cuves de carburant miniatures – contre des hackers.

Chaque école dispose d'un système autonome, ayant son propre réseau de contrôle et de gestion complet et réaliste. Chaque équipe se connecte à distance, depuis son école, de façon sécurisée pour pouvoir superviser et administrer le système dont elle aura la charge. Des caméras permettent aux participants de voir en temps réel si leurs cuves débordent ou se vident.
Les maquettes des cuves sont installées à l'École militaire, visibles par tous les auditeurs du colloque et les scores seront affichés régulièrement dans le lieu de l'exposition et en amphi Foch.
L'école qui maintient un niveau élevé de ses cuves le plus longtemps possible, est déclarée gagnante. Les résultats seront donnés le 24 septembre, à 14h00, par l'officiel général Cyber, l'amiral Arnaud Coustillière, en amphi Foch.

Le **Défi #CyberDefense** rassemble 50 élèves issus d'écoles d'ingénieurs civiles spécialisées en sécurité informatique (EPITA, ESGI, Telecom ParisTech, Telecom SudParis, ESIEA, Université Paris 6). La compétition est lancée à 9h00, le 24 septembre et les participants auront 3 heures pour trouver la vingtaine de mini-challenges qui leur sont proposés dans la plateforme de jeu. Les exercices couvrent 4 domaines qui sont : l'investigation numérique, la cryptographie, la stéganalyse et la rétroconception.

Cette épreuve doit tester, dans un format différent de **#Defnet 2015**, le modèle de réserve opérationnelle de cyberdéfense en cours de déploiement.

À chaque bonne réponse, les candidats gagnent un nombre de points qui dépend du niveau de difficulté du mini-challenge réalisé. Les résultats seront donnés le 24 septembre à 14h en amphi Foch, par l'officier général Cyber, le vice-amiral Arnaud Coustillière.

La conception et le pilotage ont été conduits par la DGA, le financement a été assuré par l'EMA et la réalisation a été menée par la société SYSDREAM.

@Defense_Gouv / #CyberDefense

#CyberDefense : les industriels en première ligne

Pour cette première édition de #CyberDefense, le ministère de la Défense peut compter une nouvelle fois sur la mobilisation et le soutien des industriels français, en particulier d'AIRBUS Defence & Space, partenaire principal de l'évènement et acteur européen incontournable en matière de cyberdéfense. En regroupant 18 sociétés partenaires, grands comptes comme PME innovantes, #CyberDefense montre le dynamisme et la capacité d'innovation de l'écosystème français en matière de lutte contre les cybermenaces auxquelles doivent faire face l'ensemble des forces armées.

À l'image de THALES, partenaire Platinum, ATOS, SOPRA-STERIA et COFELY INEO, le soutien de grands groupes internationaux spécialistes du monde de la Défense illustre pleinement la montée en puissance des enjeux liés au combat numérique. Ces derniers ont érigés en priorité nationale depuis le *Livre blanc sur la défense et la sécurité nationale* de 2013.

Fort de son dispositif d'aide au financement en matière de R&D, la Direction générale de l'armement (DGA), grâce à son programme RAPID (Régime d'appui aux PME pour l'innovation duale), participe au développement de solutions innovantes. Déclinables au monde de l'entreprise, celles-ci permettent aujourd'hui à des sociétés comme AMOSSYS, QUARCKSLAB ou FIDENS d'accélérer leur développement en contribuant au renforcement des capacités techniques et technologiques du ministère. La présence du groupement HEXATRUST et la participation de 6 de ses membres témoignent par ailleurs du dynamisme des PME innovantes françaises et de leurs ambitions internationales : BERTIN, PRIM'X, OPENTRUST, ILEX, SENTRYO et DENYALL. Créé en 2012 à l'initiative du ministre de la Défense et maillon essentiel des compétences françaises en matière de cyberdéfense, le Pôle d'excellence cyber fédère expertises académiques mais également solutions techniques développées par des PME, à l'image de SECURE-IC et de DIATEAM

Liste complète des exposants :

AIRBUS DEFENCE & SPACE

THALES

Atos

COFELY INEO GDF SUEZ

sopra steria

AMOSSYS

bertin

denyall

diateam

fidens

ilex

NEXTEL

OPENTRUST

PRIM'X

QUARKSLAB

SECURE-IC

sentryo

TETRANE

Informations pratiques

Accréditations : Centre de presse de la DICoD
presse@dicod.defense.gouv.fr
01 44 42 54 02

Officier de presse : Capitaine Stéphane Azou
06 08 47 32 01

Entrée des journalistes : 5, place Joffre 75007 Paris