DOSSIER DE PRESSE

FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ

LILLE - 28-30 janvier 2020

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

Sommaire

Le ministère des Armées au Forum international de la cybersécurité (FIC)

Vu l'importance croissante de la cybersécurité pour la protection de notre pays, la ministre des Armées, Florence Parly, a souhaité placer nos armées à la pointe dans ce domaine. La Loi de programmation militaire (LPM) 2019 – 2025 renforce ainsi les moyens alloués à ce secteur avec 1,6 Md€ et 1 000 cybercombattants supplémentaires.

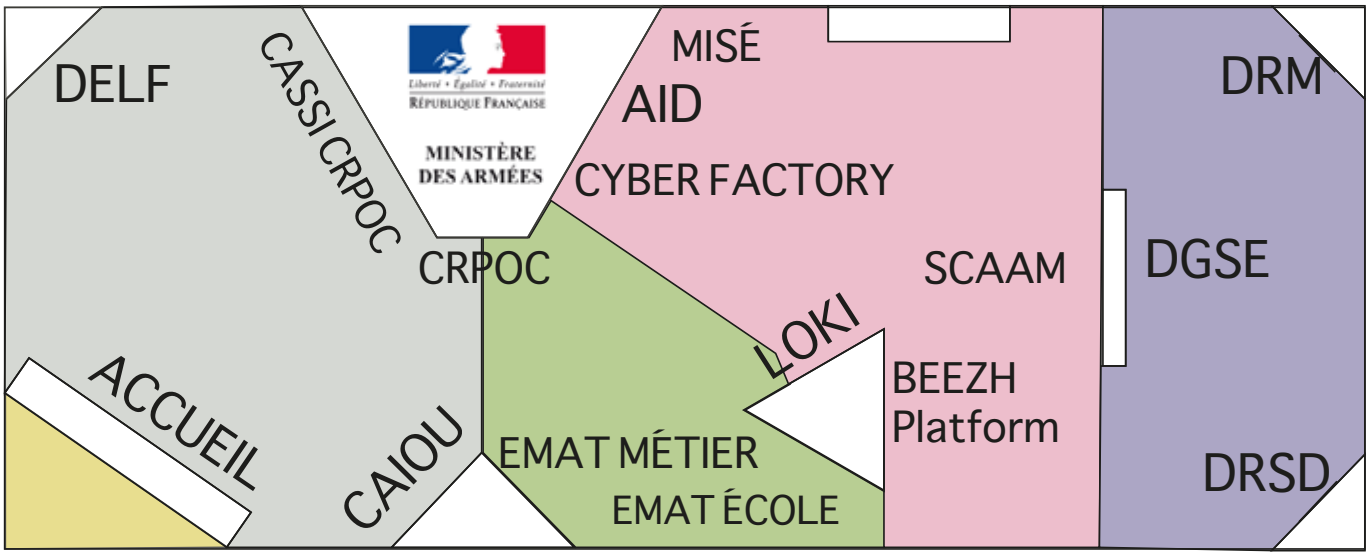
Partenaire historique de cet événement, le ministère des Armées s'associe chaque année au Forum international pour la cybersécurité (FIC). Le FIC s'est imposé comme un rendez-vous incontournable, en France et en Europe, en matière de cybersécurité et de confiance numérique. Lors de l'édition 2019, plus de 10 000 visiteurs issus de 80 pays sont venus à la rencontre des 400 partenaires présents.

La 12e édition du FIC se tient à Lille du 28 au 30 janvier 2020 avec pour thème « Replacer l'humain au cœur de la cybersécurité ». L'accent est mis sur la place de l'utilisateur qui ne doit plus être uniquement vu comme une menace mais également comme une réponse aux défis du cyber. Ce basculement implique de lui redonner une place centrale en repensant les processus, les usages et les interactions homme-machine pour privilégier l'expérience utilisateur.

Situé dans la partie centrale du Grand Palais, le stand du ministère des Armées accueille les différents acteurs cyber du ministère au sein de six espaces :

- accueil / recrutement ;
- zone d'échange ;
- zone « Anticiper et innover » ;
- zone « Renseigner » ;
- zone « Préparer les forces » ;
- zone « Combattre dans le cyberespace ».

Le stand du ministère des Armées au FIC



Combattre dans le cyberespace

DELF : Dispositif Extensible d'Analyse des Fichiers

CASSI CRPOC : Centre d'Audit de la Sécurtié des Systèmes d'Information

CAIOU : Connaissance Active des Impacts Opérationnels Utiles

Préparer les Forces

CRPOC : Centre de réserve et de préparation opérationelle de Cyberdéfense

EMAT ÉCOLE : État-major de l'Armée de Terre

EMAT METIER : État-major de l'Armée de Terre

Anticiper et innover

AID : Agence Innovation Défense

CYBER FACTORY : Projet Glimps

LOKI : Deceptive Technology Sesame IT

BEEZH Platform : Projet Amossys

SCAAM : Intelligence Artificielle

MISÉ : Intelligence Artificielle

Renseigner

DGSE : Direction Générale de la Sécurtié Extérieure

DRM : Direction du Renseignement Militaire

DRSD : Direction du Renseignement et de la Sécurtié de la Défense

Les organismes présents sur le stand du ministère des Armées

Le Commandement de la cyberdéfense (COMCYBER)

Placé sous l'autorité directe du chef d'état-major des armées, le Commandement de la cyberdéfense (COMCYBER) est responsable de la manœuvre cyber globale des armées.

Créé en 2017, implanté à Paris et à Rennes, 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 et la conduite des opérations militaires dans l'espace numérique ;
- La préparation de l'avenir en matière de 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 cybercombattants. Il dispose également de la Réserve de cyberdéfense.

FOCUS : SIGNATURE DE LA CONVENTION CYBER AVEC LES INDUSTRIELS

Florence Parly, ministre des Armées, a signé, le 14 novembre 2019, une convention cyber avec les huit maîtres d'œuvres industriels et principaux équipementiers du ministère : Airbus, Ariane Group, Dassault Aviation, MBDA, Naval Group, Nexter, Safran et Thales.

- Lors de l'édition 2019 du FIC, Florence Parly a plaidé en faveur d'un engagement mutuel fort entre le ministère des Armées et les industriels de défense, en rappelant l'importance de construire en toute confiance la chaîne de soutien (supply chain) de défense.
- Cette convention a été rédigée par le COMCYBER et la DGA, en coordination avec l'Agence nationale de sécurité des système d'information (ANSSI) et la Direction du renseignement et de la sécurité de la défense (DRSD).
- La signature de cette convention a nécessité la mise en place de groupes de travail autour de 4 piliers :
  - le partage de l'information au sein d'un cercle de confiance ;
  - l'évolution de l'organisation et l'établissement d'une gouvernance partagée ;
  - l'acculturation et la sensibilisation au cyber ;
  - la volonté commune de maîtriser les risques cyber sur l'ensemble de la chaîne de soutien de défense.

La Direction générale de l'armement (DGA)

Force d'expertise, d'essais et d'ingénierie au sein du ministère des Armées, la Direction générale de l'armement (DGA) a pour missions d'équiper les armées de façon souveraine, de préparer le futur des systèmes de défense, de promouvoir la coopération européenne et de soutenir les exportations.

Pour accompagner la montée en puissance de la cyberdéfense érigée en priorité nationale dans la LPM, la DGA se fixe deux priorités :

- maintenir un haut niveau d'expertise étatique ;
- garantir une Base industrielle et technologique de défense (BITD) dotée des compétences clé en matière de cybersécurité.

À cette fin, la DGA, en lien avec l'Agence de l'innovation de défense (AID), a mis en place une stratégie basée sur l'innovation et le renforcement de synergies avec les acteurs industriels et académiques. Couveuse d'entreprises, espace de travail collaboratif ouvert aux start-up, PME et chercheurs, dispositifs contractuels plus souples, etc. la DGA a musclé son dispositif cyber pour maintenir les armées à la pointe de la cybersécurité et gagner la bataille du numérique.

La DGA s'appuie pour cela sur le savoir-faire du centre d'expertise DGA Maîtrise de l'information et sur la Cyberdéfense Factory basée à Rennes, relai local de l'AID.

DGA Maîtrise de l'information, centre d'expertise et d'essais unique en Europe

La DGA est l'expert technique référent du ministère des Armées en matière de cybersécurité. De l'anticipation de la menace à la mise en œuvre de cyber-solutions pour les armées et les hautes autorités de l'État, elle assure, depuis la conception d'algorithmes

cryptographiques jusqu'aux architectures sécurisées de systèmes d'armement complets :

- le développement et l'évaluation de produits de cybersécurité ;
- la prise en compte de la cybersécurité dans tous les programmes d'armement ;
- le développement des capacités de lutte informatique offensive au profit des armées : en raison de la sensibilité et de la dynamique du domaine, les équipes du COMYBER et les équipes cyber de la DGA travaillent en étroite coopération à l'élaboration et à la mise en œuvre d'une feuille de route capacitaire ;
- 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.

Pour disposer d'une capacité d'expertise à la hauteur des enjeux majeurs portés par la cyberdéfense, la DGA poursuit le recrutement sur le site de DGA Maîtrise de l'information d'ingénieurs de haut niveau, spécialisés dans l'analyse et la prévention des attaques informatiques. 100 nouveaux experts en cybersécurité rejoindront la DGA en 2020 pour atteindre un effectif de 900 en 2025.

Le centre d'expertise et d'essais, implanté à Bruz (35), compte 1 450 agents, dont 80% d'ingénieurs.

FOCUS : LA CYBERDÉFENSE FACTORY

Créée par la DGA en octobre 2019, la Cyberdéfense Factory, lieu d'échange pour capter le meilleur de l'innovation civile, vient d'accueillir une première start-up. Fondée par quatre anciens ingénieurs de la DGA, la société GLIMPS compte sur la Cyberdéfense Factory pour booster le développement de son innovation, présentée sur le stand du ministère.

Cet espace inédit en France permet aux start-up, aux PME et aux universitaires de travailler au contact des experts de la DGA et des opérationnels des armées sur les sujets de cybersécurité. Au cœur de ce plateau collaboratif, la DGA met à disposition un gisement de données, appelé datalake. Tous les acteurs peuvent accéder à des données d'intérêt cyber pour tester des solutions innovantes et développer de nouveaux algorithmes. L'objectif est d'accélérer le développement de cybersolutions innovantes au profit du COMCYBER. Implantée dans la région rennaise et coordonnée par l'AID, la Cyberdéfense Factory est une antenne de l'Innovation Défense Lab.

L'Agence de l'innovation de défense (AID)

AGENCE INNOVATION DÉFENSE

Placée sous la responsabilité du Délégué général pour l'armement (DGA), l'Agence de l'innovation de défense (AID) a été créée le 1er septembre 2018 par Florence Parly, ministre des Armées. Dirigée par Emmanuel Chiva, l'AID doit inventer de nouveaux modes d'intervention et outils pour favoriser notamment les expérimentations rapides.

Résolument tournée vers l'innovation civile, l'agence doit nouer des partenariats avec les écosystèmes les plus en pointe, 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 LPM 2019-2025.

Cette nouvelle agence implique toutes les composantes du ministère, et notamment les armées, dans sa gouvernance. Elle est tournée vers l'Europe et tire pleinement parti de l'opportunité qu'est le Fonds européen de défense (FED).

En savoir plus : *www.defense.gouv.fr/aid*

La Direction générale de la sécurité extérieure (DGSE)

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Rattachée au ministère des Armées, la Direction générale de la sécurité extérieure (DGSE) est un service spécial menant des actions de renseignement à l'étranger. La DGSE a pour mission, hors du territoire national, de rechercher, collecter, exploiter et mettre à la disposition des autorités françaises des renseignements relatifs aux enjeux géostratégiques et aux menaces susceptibles d'affecter la Nation.

Elle contribue à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et menaces.

La DGSE est un service intégré qui maîtrise la totalité des modes de recueil de renseignement. En constante évolution, elle est forte de près de 7 000 personnes et composée à 77 % de civils.

La DGSE participe directement à la mise en place de capacités techniques basées sur les meilleures technologies du moment. Confrontée quotidiennement à la transformation numérique de notre société, la DGSE s'appuie sur des technologies et des infrastructures innovantes. Elle dispose d'un réseau de télécommunications mondial, d'une puissance de calcul d'envergure et de nombreux autres systèmes.

Elle recrute des femmes et des hommes prêts à relever les défis techniques parmi une grande diversité de métiers : cryptologie, interception, big data, supercalculateur, SSI, développement, IoD (Internet des Objets ou IoT - Internet of Things), etc.

La Direction du renseignement de la sécurité de la défense (DRSD)

Dans le cyberespace, la Direction du renseignement de la sécurité de la défense (DRSD) identifie les vulnérabilités et les menaces susceptibles de porter atteinte aux personnes, matériels et informations sensibles du ministère des Armées et des entreprises de défense.

Elle recueille, analyse et diffuse du Renseignement de contre-ingérence, notamment d'origine cyber (ROC) et d'intérêt cyber (RIC). Celui-ci permet d'informer les hautes autorités de l'État sur les menaces susceptibles d'affecter les intérêts de la défense, le potentiel scientifique et technologique de la Nation, ainsi que la sécurité nationale.

Elle s'appuie sur ses moyens propres et innovants (recherche humaine et technique, investigations numériques, etc.) tout en travaillant en étroite collaboration avec ses partenaires (ANSSI, CALID ou autres acteurs du renseignement).

Présente à travers le monde, la DRSD recrute des profils variés (*data scientist,* chiffreur, expert en cyberprotection, SSI, etc.) et propose des parcours de carrière aux experts du domaine cyber.

En savoir plus : *www.drsd.defense.gouv.fr*

La Direction du renseignement militaire (DRM)

Créée en 1992, la Direction du renseignement militaire (DRM) est le service de renseignement des armées. Placée sous l'autorité du chef d'état-major des armées, elle a vocation à éclairer la prise de décision autonome des hautes autorités politiques et militaires.

La DRM apporte une capacité d'anticipation stratégique et une autonomie d'appréciation de situation sur tous les sujets au cœur desquels les armées sont ou pourraient être engagées. Elle appuie les forces en fournissant le renseignement nécessaire à la planification et à la conduite des opérations. La complémentarité de ses capteurs lui permet d'agir sur tout le spectre des menaces.

La DRM regroupe 2 000 agents militaires ou civils, d'active ou de réserve. Elle dispose de cinq centres spécialisés et d'un centre de formation concourant à son autonomie d'action.

En outre, elle coordonne fonctionnellement les moyens issus des trois armées, représentant 8 000 hommes et femmes.

La DRM travaille également en lien avec les services de renseignement français et étrangers.

Les temps forts du ministère des Armées au FIC

PROGRAMMES

Dans le programme global du Salon :

Mercredi 29 janvier 2020

11h30 – 13h : atelier « L'investigation numérique à l'épreuve des avancées technologiques »

13h45 – 15h15 : atelier « Détection avancée : au-delà du discours marketing, quelle scalabilité* ? »

15h15 – 16h15 : table ronde des cyber commandeurs « Enjeux technologiques de la cyberdéfense militaire »

17h – 19h : « Intelligence artificielle : je t'aime, moi non plus », séance plénière en présence du général Didier Tisseyre, commandant le COMCYBER

** capacité d'un produit à s'adapter à un changement d'ordre de grandeur de la demande*

Jeudi 30 janvier 2020

11h – 15h : challenge « FORENSIC EPITA/COMCYBER »

12h30 : remise du prix « *Strategy Challenge* 2020 » par le COMCYBER

16h : intervention de l'amiral Arnaud Coustillière, directeur général de la DGNUM, « Quel agenda technologique et industriel pour rétablir la souveraineté numérique européenne ? »

Sur la zone d'échange du stand du ministère des Armées :

Mardi 28 Janvier 2020 :

10h30, 14h, 15h, 16h, 17h : « Intelligence Artificielle et détection », DGA

11h – 12h : remise du prix du défi « *Deceptive Security* »

Mercredi 29 Janvier 2020 – Journée innovation

10h et 14h50 : « L'AID accélère votre projet d'innovation cyber d'intérêt défense », AID

10h10 et 15h : « La Cyberdéfense Factory, un hébergement et un *datalake* cyber pour les projets innovants », DGA

10h20 et 13h30 : « Analyser les vulnérabilités et les malwares les plus complexes », Société TETRANE, projet REVEN

10h40 et 13h50 : « Anticiper les menaces sur les implémentations de cryptographie », Société ESHARD, projet SCATTER

11h et 14h10 : « Protection maîtrisée contre des cyberattaques avancées », Société TECLIB, projet MASSE

11h20 et 14h30 : « Co-ingénierie cybersécurité et sûreté de fonctionnement », Société ALL4TEL, projet COSS2

9h - 19h : échanges libres avec les experts de l'AID.

Jeudi 30 Janvier – Journée recherche

9h20 et 13h30 : « Le Pôle de Recherche Cyber, un acteur majeur de la recherche en cybersécurité », DGA

9h40 et 13h50 : « Et si le *cloud* devenait l'endroit le plus sécurisé pour vos données sensibles ? » Société SCILLE, projet PARSEC

10h et 14h10 : « Quelle confiance peut-on placer dans les plateformes matérielles qui exécutent nos applications ? », CENTRALESUPELEC

10h20 et 14h30 : « Visualiser une intrusion parmi des millions d'évènements », CENTRALESUPELEC

10h40 et 14h50 : « Quelles solutions cryptographiques face à la menace de l'ordinateur quantique ? », université Rennes 1

11h et 15h10 : « Comment détecter les intrus sur votre réseau grâce aux parasites qu'ils laissent à leur insu », DGA et CEA

11h20 et 15h30 : « L'AID accélère votre projet d'innovation cyber d'intérêt défense », AID

11h30 et 15h40 : « La Cyberdéfense Factory, un hébergement et un *datalake* cyber pour les projets innovants », DGA

Focus sur trois rendez-vous

Signature d'une convention entre le COMCYBER et l'École pour l'informatique et les techniques avancées (EPITA) – Jeudi 30 janvier à 10h30

Le général de division aérienne Didier Tisseyre, COMCYBER, et Joël Courtois, directeur de l'EPITA, concrétisent plus de six années de collaboration à travers la signature d'une convention de partenariat lors du FIC. S'inscrivant dans la continuité des actions menées depuis 2014 entre l'EPITA et le COMCYBER pour développer les compétences des jeunes talents, la signature de cette convention illustre la volonté du ministère des Armées de soutenir la filière nationale de cyber. Chaque année, le COMCYBER coopère avec les différents acteurs de l'enseignement supérieur à travers l'exercice de cyberdéfense DEFNET, mais également à travers des journées dédiées à la présentation de ses missions.

L'EPITA, avec son implantation dans toute la France, forme actuellement plus de 3 000 étudiants à devenir ingénieurs informaticiens, tous sensibilisés aux problèmes cyber.

Cette convention formalise l'engagement et l'investissement du COMCYBER et de l'EPITA à travailler conjointement dans la durée et à développer un partenariat gagnant/gagnant autour du recrutement, du rayonnement et des projets techniques.

Concours *Strategy Challenge* 2020, parrainé par le COMCYBER – Jeudi 30 janvier à 12h30

Le *Strategy Challenge* est un concours unique en son genre, conçu pour permettre aux étudiants de toutes les disciplines académiques de mieux comprendre les défis politiques liés aux cyber crises. À la fois expérience d'apprentissage interactif et exercice de scénario de compétition, il invite les équipes à réagir à une cyberattaque évolutive et réaliste et à analyser la menace qu'elle représente pour les intérêts nationaux, internationaux et privés.

Le concours a déjà mobilisé plus d'un millier d'étudiants d'universités aux États-Unis, en Europe, dans l'Indo-pacifique et au Moyen-Orient. Le *Strategy Challenge* donne aux étudiants une opportunité unique d'interagir avec des mentors experts et des professionnels de haut niveau du domaine cyber et d'écouter leurs retours, tout en développant des compétences précieuses en analyse et en présentation politiques. Les équipes sont jugées en fonction de leurs réponses politiques, de leurs processus décisionnels et de leur présentation orale.

Défi cyber « *Deceptive Security* » : présentation des deux projets finalistes et annonce du vainqueur pendant le salon – Mardi 28 janvier à 11h

Organisé par la DGA en relation avec le COMCYBER et l'AID, le défi cyber « Deceptive Security » a été lancé en juin 2019. Il vise à faire émerger une solution innovante et expérimentable par les forces armées, pour faciliter l'analyse des cyberattaques visant les réseaux du ministère des Armées. Dans un marché dominé par de grands acteurs internationaux, la DGA veut favoriser ainsi une innovation portée par une start-up ou une PME/ETI française.

Les finalistes de ce défi sont les PME AMOSSYS et SESAME IT. Le vainqueur sera annoncé pendant le salon et pourra tester son prototype au sein du ministère des Armées.

Les projets sont à découvrir sur le stand du ministère.

Piéger un cyberattaquant pour observer et comprendre son mode opératoire : c'est sur ce principe que reposent les innovations développées par les PME AMOSSYS et SESAME IT.

- Le produit BEEZH Platform, développé par la PME AMOSSYS, est ainsi capable de reconstituer de manière très réaliste un système d'information, laissant penser à l'attaquant qu'il a réussi à pénétrer le réseau informatique ciblé. Sa particularité ? Les nombreuses possibilités de personnalisation et la capacité à générer en permanence de l'activité utilisateur pour produire un système crédible et cohérent.
- Le projet LOKI, développé par la PME SESAME IT, consiste à leurrer les cyberattaquants en les attirant dans un réseau parallèle. Comment ? En déployant un réseau de leurres réalistes et crédibles. La technologie permet de reproduire tous les types de réseaux, de manière automatisée. Elle permet de détecter en temps réel une tentative d'intrusion et offre aussi la possibilité de mener des actions offensives, en disséminant des fichiers piégés dans le réseau de leurres.

Informations pratiques

ADRESSE

Lille Grand Palais

1 boulevard des Cités Unies

59777 Lille – Euralille

HORAIRES DU SALON

Mardi 28 janvier 2020 de 10h00 à 18h00

Mercredi 29 janvier 2020 de 9h00 à 19h00

Jeudi 30 janvier 2020 de 9h00 à 18h00

CONTACTS MEDIA

DICoD / Centre Media – 09 88 67 33 33

media@dicod.fr

Retrouvez plus d'informations sur le site du FIC :

https://www.forum-fic.com

LE MINISTÈRE DES ARMÉES

ENGAGÉ POUR LA DÉFENSE DE LA FRANCE ET DES FRANÇAIS

Plus de 30 000 militaires assurent au quotidien la sécurité de nos concitoyens en France et à l'étranger, dont 13 000 sur le territoire national et environ 6 000 déployés en opérations extérieures

TOURNÉ VERS L'AVENIR

4,9 milliards d'euros de Recherche & Développement, dont 758 millions par an consacrés aux études amonts, un chiffre qui s'élèvera à 1 milliard d'euros dès 2022

ACTEUR ÉCONOMIQUE MAJEUR

35.9 milliards d'euros de budget en 2019 soit le 2e budget de l'État après celui de l'Éducation nationale
19.5 milliards d'euros pour l'équipement des forces
1,84 % du PIB en 2019 avec pour objectif 2 % du PIB en 2025
Les entreprises de Défense représentent 20 % des exportations de la France
26 000 PME et ETI sont fournisseurs directs du ministère des Armées

À HAUTEUR D'HOMME

26 000 recrutements par an dont 4 500 civils
270 000 hommes et femmes dont 208 000 militaires et 62 000 civils
20,7 % de femmes
38 000 réservistes opérationnels sous contrat

2e ACTEUR CULTUREL DE L'ÉTAT

16 musées, 160 monuments classés (3 millions de visiteurs par an),
3 millions de photos et 21 000 films d'archives couvrant 4 siècles d'histoire

1er ACTEUR MÉMORIEL DE L'ÉTAT

275 nécropoles nationales, 10 hauts lieux de la mémoire nationale,
2 200 carrés militaires, un milier de lieux de sépulture dans 80 pays,
lieux de commémoration et de transmission de la mémoire combattante

Centre Media du ministère des Armées
Tél. : 09 88 67 33 33
media@dicod.fr

Ministère des Armées
@Defense_gouv
@ministeredesarmees