MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

« Le nouveau monde numérique n'est plus le fruit de l'imagination de quelques auteurs iconoclastes. Le nouveau monde numérique, le nouveau monde cyber n'est plus une source de fantasme ou de débat. Le nouveau monde cyber, c'est aujourd'hui et ce n'est pas près de s'arrêter.

Tout, aujourd'hui, est connecté. Tout. Depuis nos téléphones jusqu'à nos vêtements, en passant par nos voitures et même nos brosses à dent. Tout collecte les données, les traite, les classe, les analyse. On a pensé que le numérique s'arrêterait à quelques objets précis, nous avions tort : 'l'internet of things' est aujourd'hui devenu 'l'internet of everything'.

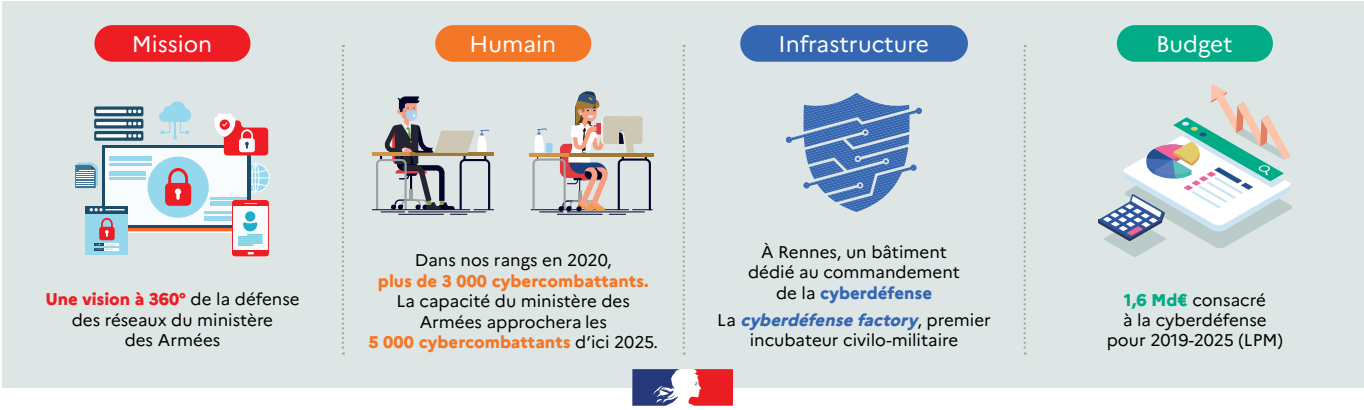
Mais nos vies changent, nos modes de vie s'adaptent et avec, nos modes de combat. »

Florence Parly, ministre des Armées,
lors de l'édition 2018 du FIC

Sommaire

Partie 1 :

LA CYBERDÉFENSE



Désormais le monde est interdépendant et interconnecté. Sa transformation numérique fait émerger de nouveaux usages et de nouvelles menaces, permanentes et en évolution continue.

Pour y répondre et assumer pleinement son rôle de cyberpuissance, le ministère des Armées a fait de la cyberdéfense une de ses priorités et un enjeu stratégique. La loi de programmation militaire (LPM) 2019-2025 y consacre 1,6 milliard d'euros.

Le ministère s'est donné les moyens de construire une cyberdéfense en se dotant, en 2019, d'une doctrine militaire de Lutte informatique offensive (LIO) et en renforçant sa politique de Lutte informatique défensive (LID).

Pour assurer la protection et la défense des systèmes d'information et de communication du cyberespace, le ministère des Armées dispose d'une organisation robuste avec des femmes et des hommes qualifiés ainsi que des infrastructures dédiées.

Glossaire du cybercombattant

Le cyberespace : espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques (Source : Autorité nationale en matière de sécurité et de défense des systèmes d'information, ANSSI).

La cyberdéfense : ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels (Source : ANSSI).

Les cyberattaques : acte malveillant de piratage d'informations dans le cyberespace. Les cyberattaques peuvent être l'action d'une personne isolée, d'un groupe ou d'un État. Elles incluent la désinformation, l'espionnage électronique visant à affaiblir l'avantage compétitif d'une nation, la modification clandestine de données sensibles sur un champ de bataille ou la perturbation des infrastructures critiques d'un pays. Ces actes peuvent être motivés par l'appât du gain ou par des intérêts politiques.

1. Les missions de la cyberdéfense

Prévenir, pour faire prendre conscience aux utilisateurs du risque représenté par la numérisation de leurs équipements ou des organisations qu'ils servent.

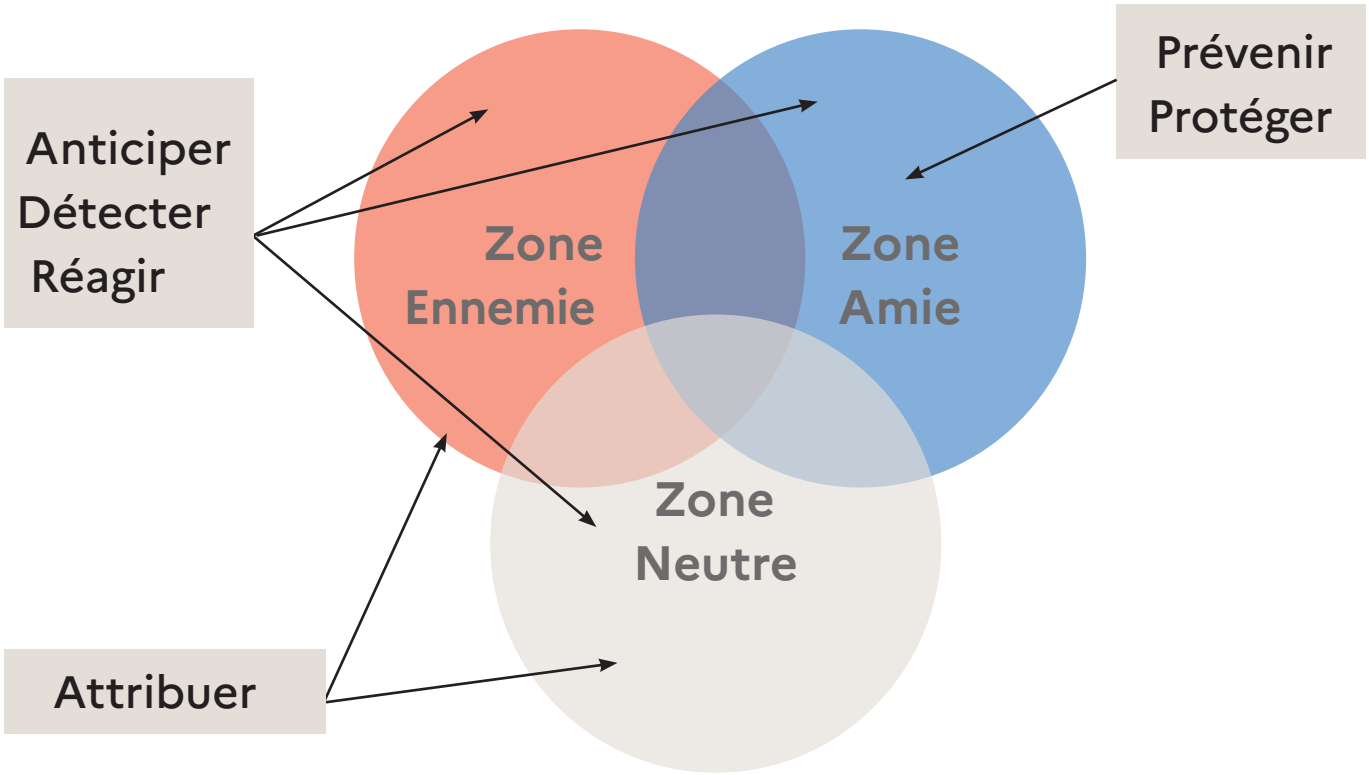
Anticiper, pour évaluer en permanence les probabilités de cyberattaques et prendre des mesures préventives lorsque la menace paraît suffisamment forte.

Protéger, pour diminuer la vulnérabilité de nos systèmes informatiques en compliquant la tâche des attaquants potentiels et en facilitant la détection des cyberattaques. La protection est nécessaire tout au long du cycle de vie des systèmes.

Détecter, pour rechercher des indices d'une éventuelle cyberattaque en cours. Le ministère des Armées complète ses informations en sollicitant ses partenaires nationaux et internationaux.

Réagir, pour résister à une cyberattaque afin qu'elle n'empêche pas la poursuite des activités du ministère.

Attribuer, pour identifier l'auteur d'une cyberattaque par des preuves ou un faisceau d'indices. Les services de renseignement sont au cœur de ce processus de recueil d'indices d'attribution.



2. Les cybercombattants

Les cybercombattants travaillant au ministère des Armées possèdent un haut niveau d'expertise grâce aux formations et aux entraînements reconnus dans le civil (exercices DEFNET, Locked Shields). Leurs compétences, leurs qualifications, leurs possibilités de progression et la richesse de leurs parcours sont de véritables atouts. La LPM prévoyait près de 1100 recrutements supplémentaires. Compte-tenu des conclusions de l'actualisation de la revue stratégique, le vivier de cybercombattants sera renforcé de 770 recrutements supplémentaires, portant à environ 1900 le nombre de nouveaux cybercombattants qui rejoindront le ministère des Armées entre 2019 et 2025.

Partie 2 :

LE FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ (FIC)

L'édition 2021 du Forum international de la cybersécurité (FIC) se déroulera au Grand Palais de Lille (59) les 7, 8 et 9 septembre. Il aura pour thème « une cybersécurité collective et collaborative ».

Comme chaque année, le ministère des Armées s'associe à ce rendez-vous incontournable des acteurs de l'écosystème européen de la cybersécurité.

Le ministère des Armées recrute environ 1 900 cybercombattants d'ici 2025 pour soutenir les missions de renseignement, de protection, de défense et d'action dans le cyberespace.

Le recrutement s'effectue sous différents statuts (militaire, civil, réserviste), à tout type de niveau, notamment pour les passionnés du numérique. En effet, les profils recherchés sont divers : expert ou manager, premier emploi ou au titre d'un parcours professionnel diversifié... Ces postes couvrent un large spectre d'activités et des missions opérationnelles variées :

- ingénierie logicielle (expression du besoin, conception, développement, etc.) ;
- administration système et sécurité ;
- sécurité des systèmes d'information (assistance, conseil, expertise) ;
- évaluation des systèmes (audit, test d'intrusion, Red team, ...) ;
- lutte informatique défensive (évaluation de la menace cyber, analyse de traces et supervision dans les SOC, forensic, reverse engineering, ...) ;
- veille sur les réseaux sociaux.

LES ORGANISMES PRÉSENTS SUR LE STAND DU MINISTÈRE DES ARMÉES

1. Le commandement de la cyberdéfense

Le Commandement de la cyberdéfense (COMCYBER), sous l'autorité directe du Chef d'état-major des armées (CEMA), est responsable de la manœuvre cyber globale des armées. Créé en 2017, implanté à Paris et à Rennes, le COMCYBER a pour missions :

- la protection des systèmes d'information de l'état-major des armées et du ministère des Armées ;
- la conception, la planification, la conduite des opérations militaires offensives et défensives 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 un vivier riche de plus de 3000 cybercombattants civils et militaires de réserve ou d'active.

Il dirige également le Centre des réserves et de préparation opérationnelle de cyberdéfense (CRPOC), acteur majeur du recrutement et de l'affectation des réservistes de cyberdéfense.

Le recrutement s'effectue sous différents statuts (militaire, civil, réserviste).

Pour postuler : ema-cyberdefense.contact.fct@intradef.gouv.fr

Focus opérations

Sous le commandement du COMCYBER, l'arme cyber est employée, au même titre que les armes conventionnelles, sur les théâtres d'opérations. Ces actions s'appuient sur la doctrine militaire de Lutte informatique offensive (LIO). Au Sahel, comme sur les autres théâtres, les armées disposent de capacités spécifiques pour appuyer les actions classiques de Barkhane, mais aussi veiller, analyser et, si besoin, neutraliser la propagande cyber des groupes armés terroristes.

DEFNET

L'exercice DEFNET mobilise et entraîne l'ensemble de la chaîne de cyberdéfense du ministère des Armées à réagir à différents incidents de grande ampleur sur les réseaux déployés en opération et sur le territoire national, dans un contexte international fictif. DEFNET est spécialement conçu pour permettre aux armées, directions et services du ministère des Armées de planifier, coordonner et mettre en œuvre des mesures défensives spécifiques en phase avec la réalité de la menace cyber (menaces ciblées et attaques simultanées).

Chaque année, DEFNET mobilise près de 260 cybercombattants sur de nombreux sites militaires en France (Brest, Istres, Paris, Rennes, Toulon…). Les réservistes opérationnels de cyberdéfense, les partenaires industriels, ainsi que l'Agence nationale de la sécurité des systèmes d'information sont également impliqués. Pour la 8e édition en mars 2021, les étudiants ont été invités à participer : le COMCYBER a organisé un « *Capture The Flag* » avec 14 écoles d'enseignement supérieur à Paris et dans le Grand Ouest.

2. La direction interarmées des réseaux d'infrastructure et des systèmes d'information

DIRISI La Direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI) est l'opérateur des systèmes d'information de la défense sous les ordres du CEMA. Elle appuie en continu (24h/24 et 7j/7) les forces armées engagées en opérations extérieures, en missions de sécurité intérieure et en exercices, en fournissant les systèmes d'information et de communication (SIC) nécessaires. Elle contribue au fonctionnement quotidien et à la modernisation du ministère des Armées.

La DIRISI est composée d'environ 7 000 personnes (60% de militaires, 40% de civils), réparties sur l'ensemble du territoire métropolitain, en outre-mer et à l'étranger.

Ses missions sont de garantir la transmission opérationnelle, d'appuyer la transformation numérique du ministère, d'assurer l'exploitation des systèmes numériques qui lui sont confiés et de fournir les équipements SIC à l'ensemble du ministère.

Partie prenante de la révolution numérique, la DIRISI a opéré sa propre transformation en réorganisant ses activités autour de cinq pôles : hébergement, développement, espace numérique de travail, réseaux transports et desserte, sécurité et administration.

Pour répondre à son besoin de compétences SIC*, elle offre à tous des opportunités dans de nombreux domaines et des possibilités d'évolution de carrière.

+d'infos

- **Offres d'emploi :** https://contractuels.civils.defense.gouv.fr/
- **Offres d'alternance :** https://stages.defense.gouv.fr/
- www.linkedin.com/company/dirisi

* Environ 200 recrutements d'ingénieurs et de techniciens par an et de nombreuses possibilités de contrats d'apprentissage de tous niveaux.

3. L'armée de Terre

Source de menaces permanentes et en évolution continue, la cybersécurité est un enjeu majeur pour l'armée de Terre. La multiplication des systèmes d'information et d'échanges ainsi que la numérisation croissante des systèmes d'armes et logistiques augmentent la surface d'exposition de l'armée de Terre aux attaques cybernétiques. L'enjeu stratégique « cybersécurité » est d'agir sur l'ensemble du continuum sécurité des systèmes, afin de garantir la supériorité opérationnelle des unités aéroterrestres.

- **l'École des transmissions (ETRS) près de Rennes** : intégrée au Commandement des systèmes d'information et de communication (COMSIC), elle assure la formation du personnel militaire et civil des armées en cybersécurité ;
- **l'Académie militaire de Saint-Cyr Coëtquidan (AMSCC)** : le mastère spécialisé « Opérations et gestion des crises en cyber défense » a pour vocation de former des experts généralistes civils et militaires des opérations cyber (cyberprotection, lutte informatique défensive, gestion de crise, etc.) ;
- **le Lycée militaire (LM) de Saint-Cyr-l'École** : le BTS « Système numérique informatique et réseaux option Cyberdéfense » permet de préparer les futurs cadres du ministère des Armées à tenir des postes d'informaticiens liés à la sécurité des systèmes informatiques.

UNE ARMÉE DE TERRE FORTE D'UNITÉS SPÉCIALISÉES

À Rennes et aux alentours :

- **le COMSIC** : contribue directement aux missions cyber et à la préparation à l'engagement des forces en opérations ;
- **la 807e Compagnie de transmissions (807e CT)** : spécialisée dans la défense des systèmes d'information, son personnel est projeté en permanence sur les théâtres d'opération extérieure ;
- **la 785e Compagnie de guerre électronique (785e CGE)** : ces 110 femmes et hommes de l'armée de Terre réalisent, entre autres, des missions d'appui à la sécurité des systèmes d'information (audits de sécurité informatique) ;
- **un Centre technique de Lutte informatique défensive (CT-LID)** : créé en 2019 le CT-LID assure la surveillance et la défense des systèmes métiers de l'armée de Terre déployés en métropole.

À Paris :

- **une Cellule de coordination de Lutte informatique défensive (C2LID)** : une dizaine de personnes veille sur l'empreinte numérique de l'armée de Terre (systèmes d'information, sites internet, etc.) et son maintien en condition de sécurité.

Le Commandement du renseignement des forces terrestres (COMRENS) à Strasbourg, créé en 2016, regroupe sous ses ordres des unités traitant de cyberdéfense :

- **Le 44e Régiment de transmissions (44e RT) à Mutzig :** Unique unité du renseignement d'origine électromagnétique (ROEM) stratégique de l'armée de Terre, il renseigne en permanence sur les cibles d'intérêt militaire prioritaires à partir du centre de guerre électronique, et arme des détachements en opérations extérieures ;

- **Le 54e Régiment de transmissions (54e RT) à Haguenau :** il est l'unique régiment de guerre électronique tactique de l'armée de Terre. Il est en mesure de générer le poste de commandement d'un Groupement de recherche multicapteur (GRM) ;

- **Le Centre du renseignement terre (CRT) à Strasbourg :** créé en 2016, il regroupe plus de 200 spécialistes du renseignement. Il permet d'optimiser les capacités d'analyse et d'exploitation de l'armée de Terre

- **785e Compagnie de guerre électronique (785e CGE) près de Rennes:** 110 femmes et hommes de l'armée de Terre, réalisant entre autres des missions d'appui à la sécurité des systèmes d'information (audits de sécurité informatique). Des formations adaptées à cet enjeu :

4. La direction générale de l'armement

Force d'ingénierie, d'expertise et d'essais au sein du ministère des Armées, la Direction générale de l'armement (DGA) a pour missions principales 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.

La DGA conduit aujourd'hui plus d'une centaine de programmes et d'opérations d'armement par an. Ils couvrent tous les domaines de la défense et répondent aux besoins opérationnels des armées : sous-marins, navires, satellites, systèmes de commandement, avions, hélicoptères, missiles, véhicules blindés, armement terrestre, armement nucléaire, etc.

Acteur majeur de la recherche et technologie de défense en France et en Europe, la DGA a la responsabilité de préparer les futurs systèmes de défense qui arriveront dans les forces dans les prochaines décennies. Son ambition : équiper les armées au meilleur niveau technologique pour leur assurer la supériorité opérationnelle et permettre à la France de conserver son indépendance.

La DGA mène ces missions depuis 60 ans dans l'objectif constant d'équiper les armées aux meilleurs standards internationaux, d'assurer la pérennité de la Base industrielle et technologique de défense (BITD) pour permettre à la France de disposer d'un modèle d'armée complet et de conserver, dans la durée, son autonomie de décision et d'action.

Être au rendez-vous technologique des armées est un impératif stratégique, opérationnel et industriel.

La direction générale de l'armement recrute :

Caractérisée par sa mixité militaires-civils, la DGA réunit plus de 10 000 femmes et hommes, de catégories professionnelles et de métiers très variés, répartis dans toute la France.

Ingénieurs, chercheurs, experts scientifiques et techniques, ouvriers et techniciens, aventuriers des nouvelles technologies, etc., la DGA réunit des talents, des personnes engagées et motivées par leur mission, capables de se dépasser et de relever tous les défis au bénéfice des forces armées.

Tous constituent un panel d'expertises dans tous les domaines, de savoir-faire, de compétences les plus pointues, capables de concevoir des objets parmi les plus complexes au monde, comme des sous-marins ou satellites, qui répondent à des défis croissants de performances et de miniaturisation.

Vous êtes techniciens, ingénieurs ? La DGA recrute, de bac+2 à bac+5 dans de nombreux domaines techniques (cybersécurité, data sciences et intelligence artificielle, optronique, systèmes de drones, systèmes de combat navals, télécommunication etc.), mais aussi fonctionnels (achats, affaires internationales ou encore qualitéproduit). Plus de 400 postes en CDI sont ouverts chaque année dans toute la France. Retrouvez les offres d'emploi sur le site Internet de la DGA. www.defense.gouv.fr/dga

Focus entreprises

LE DIAG CYBER

Mesure du plan Action PME du ministère des Armées, le « Diag Cyber », dispositif d'aide à la cybersécurisation, vise à réduire les vulnérabilités numériques des PME et des ETI de l'industrie de Défense. Il permet à une entreprise bénéficiaire de se faire financer 50% des frais de cybersécurisation.

Les entreprises désireuses de bénéficier de ce dispositif sont invitées à faire une demande en ligne sur la plate-forme :

www.demarches-simplifiées.fr/commencer/diagnostic-cyber-defense

Pour connaitre toutes les mesures du ministère des Armées spécifiquement dédiées aux PME et ETI, une seule adresse :

https://www.defense.gouv.fr/portail/enjeux2/economie-de-defense/pme-et-eti-plan-actionpme-du-ministere-des-armees

« Le ministère des Armées investit 4,5 M€ dans ce dispositif ».

LA CYBERDÉFENSE FACTORY

Lancée en octobre 2019, la « Cyber défense factory » vise à favoriser l'innovation en offrant à des chercheurs et des entrepreneurs un hébergement, l'accès à des données d'intérêt cyber et la capacité de développer et tester les solutions avec des experts et des opérationnels du ministère des Armées.

Elle joue ainsi le rôle de « couveuse d'entreprises » pour de jeunes start-ups prometteuses. Un appel à projets externe permanent est ouvert aux organismes de recherche, aux start-ups, aux PME ou encore aux ETI, seuls ou en consortium (rendez-vous sur **https://** www.defense.gouv.fr/aid/appels-a-projets/appel-a-projets-pour-la-cyber-defense-factory).

Un appel à projets interne permet également aux personnels des armées de se lancer dans une création d'entreprise. Ce lieu expérimental et unique en France, situé à Rennes, est supervisé par le commandement de la cyberdéfense, en synergie avec le centre d'expertise et d'essais DGA Maîtrise de l'information et l'Agence de l'innovation de défense.

Le premier projet accueilli fin 2019 a été porté par la société Glimps. Il a concerné le développement d'outils d'aide à l'analyse de code binaire. Fin 2020, trois nouveaux projets portés par les sociétés Malizen, LumenAI et Sahar ont intégré la Factory.

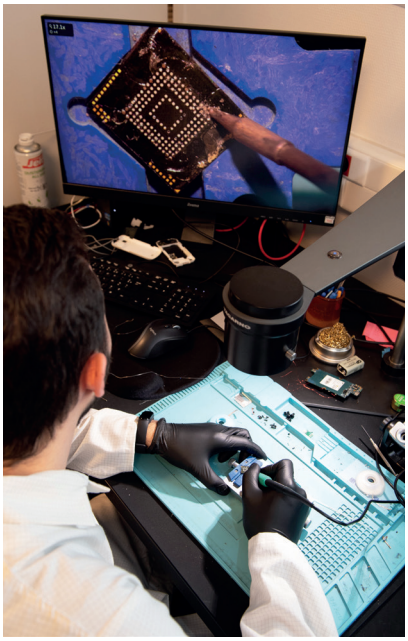
5. La direction du renseignement militaire

Créée en 1992, la Direction du renseignement militaire (DRM) est le service de renseignement des armées. Placée sous l'autorité du CEMA, 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, qui regroupe 2 000 agents militaires ou civils, d'active ou de réserve, 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.

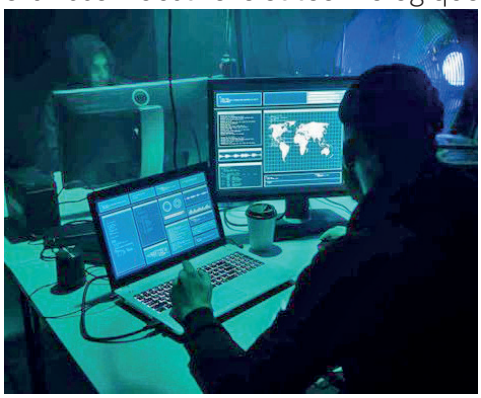
La DRM travaille également en lien avec les services de renseignement français et étrangers.

Afin de faire face à l'évolution des technologies et pour mieux s'adapter aux menaces, la DRM recrute en permanence dans de nombreux domaines. Elle assure en interne les formations de spécialités de ses agents.

https://www.defense.gouv.fr/drm/recrutement

6. La direction du renseignement et de la sécurité de la Défense

Service de renseignement du ministre des Armées, la Direction du renseignement et de la sécurité de la Défense (DRSD) alerte sur les vulnérabilités, renseigne sur les menaces, investigue sur les compromissions et contribue aux mesures de protection ou d'entrave du ministère et de la Base industrielle et technologique de la défense (BITD). Elle dispose à cette fin d'une autonomie accrue sur tout le spectre de la sécurité, y compris dans le cyberespace.



La DRSD agit comme service enquêteur au titre de la protection du secret de la défense nationale. Elle a des responsabilités propres vis-à-vis de l'industrie de défense dont elle assure la sensibilisation et contribue à certaines formations spécifiques.

La DRSD caractérise l'adversaire cyber de la sphère défense (mission « attribution »). Impliquée dans la réponse à incident, elle a créé des Éléments d'intervention cyber (EIC) pour enquêter *in situ* sur les cyberattaques, au profit de la sphère défense.

Présente à travers le monde, la DRSD recrute des profils variés et propose des parcours de carrière aux experts du domaine cyber.

www.drsd.defense.gouv.fr

7. La direction générale de la sécurité extérieure

Rattachée au ministère des Armées, la Direction générale de la sécurité extérieure (DGSE) est le service chargé de mener des actions de renseignement à l'étranger.

La DGSE a pour mission, hors du territoire national, de rechercher, exploiter et mettre à la disposition des autorités françaises des renseignements relatifs aux enjeux géostratégiques et aux menaces susceptibles d'affecter la Nation.

Service de renseignement et d'action, elle contribue à la connaissance et à l'anticipation mais aussi à l'entrave des menaces visant les intérêts français.

La DGSE est un service intégré qui maîtrise la totalité des modes de recueil de renseignement humain, technique et opérationnel. En constante évolution, elle est forte de près de 7 000 personnes et composée à 68 % de civils.

La DGSE participe directement à la mise en place de capacités techniques basées sur les meilleures technologies du moment. 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 : big data, cryptologie, interception, supercalculateur, cyberdéfense, SSI, développement logiciels, IoD (Internet des Objets ou IoT - Internet of Things), etc.

https://www.dgse.gouv.fr/fr

LE MINISTÈRE DES ARMÉES

ENGAGÉ POUR LA DÉFENSE DE LA FRANCE ET DES FRANÇAIS

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

TOURNÉ VERS L'AVENIR

5,5 milliards d'euros de Recherche & Développement, 1 milliard d'euros par an sera consacré à l'innovation à compter de 2022 soit une hausse de près de 38% par rapport à l'entrée de la Loi de programmation militaire (LPM) 2019-2025.

ACTEUR ÉCONOMIQUE MAJEUR

37,5 milliards d'euros de budget en 2020, soit le 2e budget de l'État.
12,6 milliards d'euros pour l'équipement des forces.
1,86 % du PIB en 2020, avec pour objectif 2 % du PIB en 2025.
Les entreprises de Défense représentent 20 % des exportations de la France.
26 000 Petites et moyennes entreprises (PME) et Entreprises de taille intermédiaire (ETI) en contrat avec le ministère des Armées.

À HAUTEUR D'HOMME

27 000 recrutements par an, dont 4 000 civils.
268 300 hommes et femmes, dont 21 % de femmes.
205 800 militaires et 62 500 civils.
41 000 réservistes opérationnels sous contrat.

2E ACTEUR CULTUREL DE L'ÉTAT

21 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 millier 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

FACEBOOK @Armees.gouv
TWITTER @Armees_Gouv
INSTAGRAM @Armees_Gouv
YOUTUBE Ministère des Armées
LINKEDIN Ministère des Armées

Retrouvez-nous sur **www.defense.gouv.fr**