RESSOURCES PÉDAGOGIQUES

LES ENJEUX DE SECURITE DANS LE CYBERESPACE

VU DE LA POSTURE FRANÇAISE

TABLE DES MATIÉRES

1. Présentation du Cyberespace 2
   1.1. Qu'est-ce que le cyberespace ? 2
   1.2. La vision militaire française du cyberespace 2

2. Origine et organisation du commandement de la cyberdéfense 4

3. Les opérations militaires dans le cyberespace 7
   3.1. La lutte informatique défensive (LID) 8
   3.2. La lutte informatique offensive (LIO) 9
   3.3. La lutte informatique d'influence (L2I) 11

4. Les cybercombattants 13
   4.1. Des métiers aussi divers que passionnants 13
   4.2. Brain games, serious games et wargames : la « ludification » au service de l'anticipation 14
   > DEFNET : 15
   > LOCKED SHIELDS : 15

5. Fond documentaire 16
   5.1. Références textuelles 16
   5.2. Glossaire des termes employés et des acronymes utiles à connaître 17

La présente fiche a pour objet de présenter les enjeux de sécurité dans le cyberespace du point de vue du commandement de la cyberdéfense (COMCYBER) et du ministère des Armées. Après avoir défini le cyberespace et présenté la vision militaire de ce milieu transverse, le document s'attache à décrire l'organisation du COMCYBER et son environnement, puis à synthétiser les différents domaines de lutte informatique et la spécificité des opérations militaires dans le cyberespace. Enfin, la fiche présente les cybercombattants et les enjeux spécifiques aux ressources humaines comme le recrutement ou la formation. Ce document a vocation à être exploité par des enseignants.

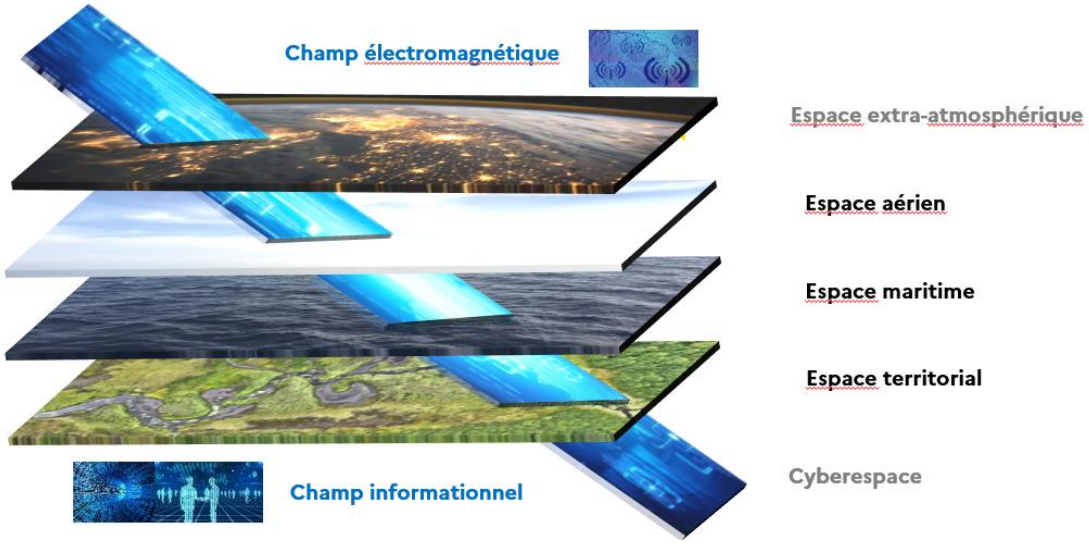
PRÉSENTATION DU CYBERESPACE

1.1. Qu'est-ce que le cyberespace ?

1.2. La vision militaire française du cyberespace

L'humanité a toujours connu des périodes de conflictualité de plus ou moins forte intensité, allant de simples tensions très localisées à des guerres à l'échelle mondiale. A l'origine purement terrestres, les conflits, au gré des avancées technologiques, se sont progressivement étendus et développés au milieu maritime avant d'évoluer vers d'autre milieux rendus désormais accessibles à l'homme. On pense naturellement au milieu aérien ou à l'espace sous-marin, mais également plus récemment au milieu extra-atmosphérique**. Le cyberespace n'échappe pas à la règle et il constitue désormais un espace de confrontation très singulier en raison de sa technicité, de son étendue et de sa transversalité avec les autres espaces de conflictualité**. La vision militaire du cyberespace est donc un peu différente de celle du monde civil et cet espace artificiel s'intègre à un schéma global plus large formalisé en cinq grands types d'espaces et deux champs tels que représentés ci-dessous :

Les différents espaces de confrontation



Le cyberespace est donc un espace transverse de communication et d'échanges favorable au progrès et un support essentiel du fonctionnement de nos sociétés et de nos États**. L'expansion du numérique a parallèlement engendré des vulnérabilités structurelles croissantes aux incidents cyber** (comme une simple panne de réseau ou un problème de connexion). **Le développement exponentiel des cyberattaques constitue également une menace prégnante pour les états, les organismes publics ou privés, mais également les citoyens.**

À ce titre, **les risques d'entrave et d'espionnage demeurent croissants vis-à-vis du système d'information de l'État.** La prise en compte de ces risques fait l'objet d'un traitement particulier dans le cas des systèmes d'information d'importance vitales[1].

Avec les réseaux sociaux, les cyberattaques ne sont pas uniquement informatiques mais elles peuvent être aussi informationnelles, à des fins d'influence.

L'Etat français a bien pris en compte la menace, et sous l'impulsion du président de la République et du gouvernement, **conduit une politique active de cybersécurité et de sécurité numérique à différents niveaux afin de rendre la société française la plus résiliente possible aux cyberattaques**.

[1] Systèmes d'information d'importance vitale : systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.

Pour prendre en compte l'ensemble de ces risques et la particularité du ministère des Armées, la définition du cyberespace militaire a été précisée. Le cyberespace militaire est donc un peu différent du cyberespace commun classique et est constitué de trois grands ensembles :

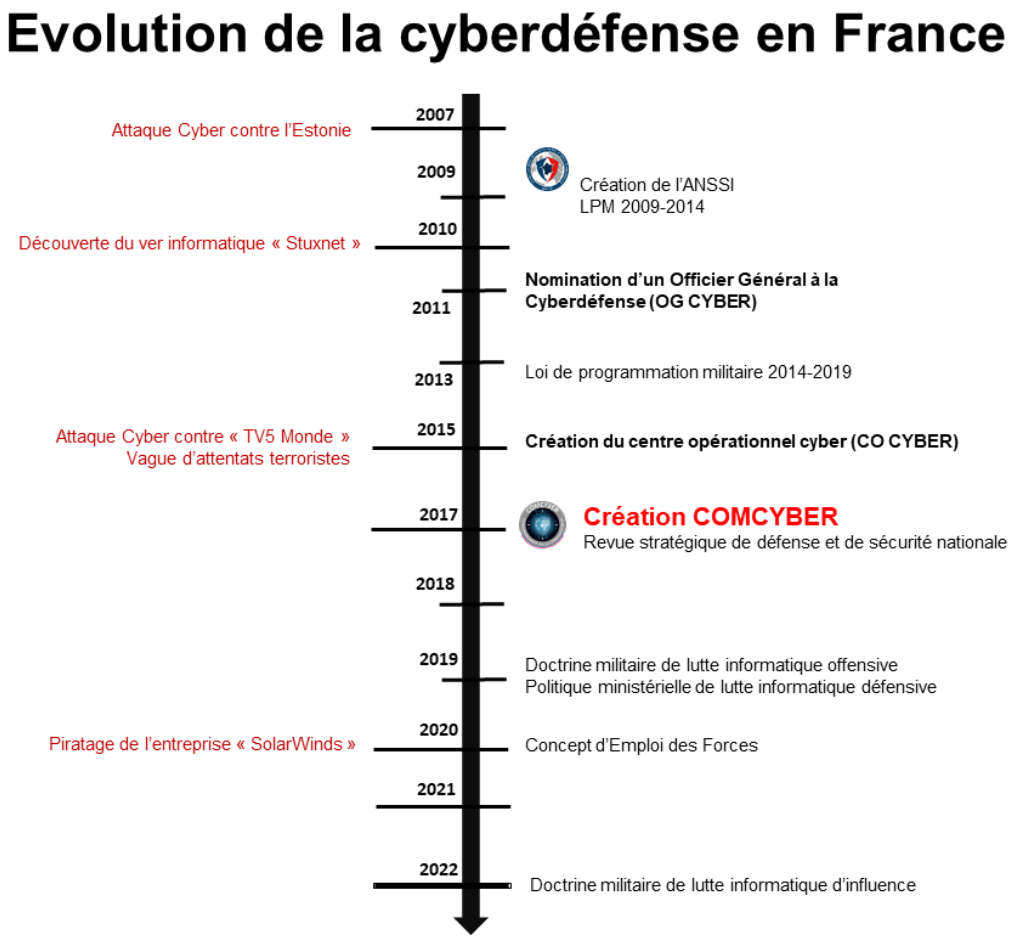
- Tout d'abord, **des systèmes informatiques et de communication**, certes militaires, mais comparable aux systèmes classiques largement déployés dans nos sociétés modernes numérisées.
- **Des systèmes d'armes**, équipement militaires très spécifique et protégés, largement différents de ce qui se fait ailleurs.
- **Des systèmes de contrôle et d'acquisition de données, commun et partagés avec de grands industriels ou partenaires fournisseurs du ministère des Armées**.

Les différents types de système du ministère des Armées

Le ministère des Armées a la responsabilité de protéger l'intégralité de ces systèmes et d'être en mesure d'agir dans tout le cyberspace, dans les zones « ami, neutre ou ennemi » (cf. *infra*).

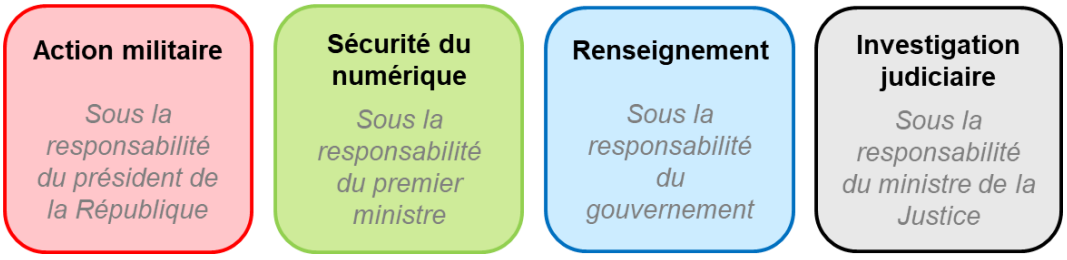
ORIGINE ET ORGANISATION DU COMMANDEMENT DE LA CYBERDÉFENSE

Depuis 2007, de nombreux événements importants sur le plan international et national ont permis, à la suite de décisions politiques majeures, de façonner et de structurer l'organisation actuelle de la cyberdéfense française.



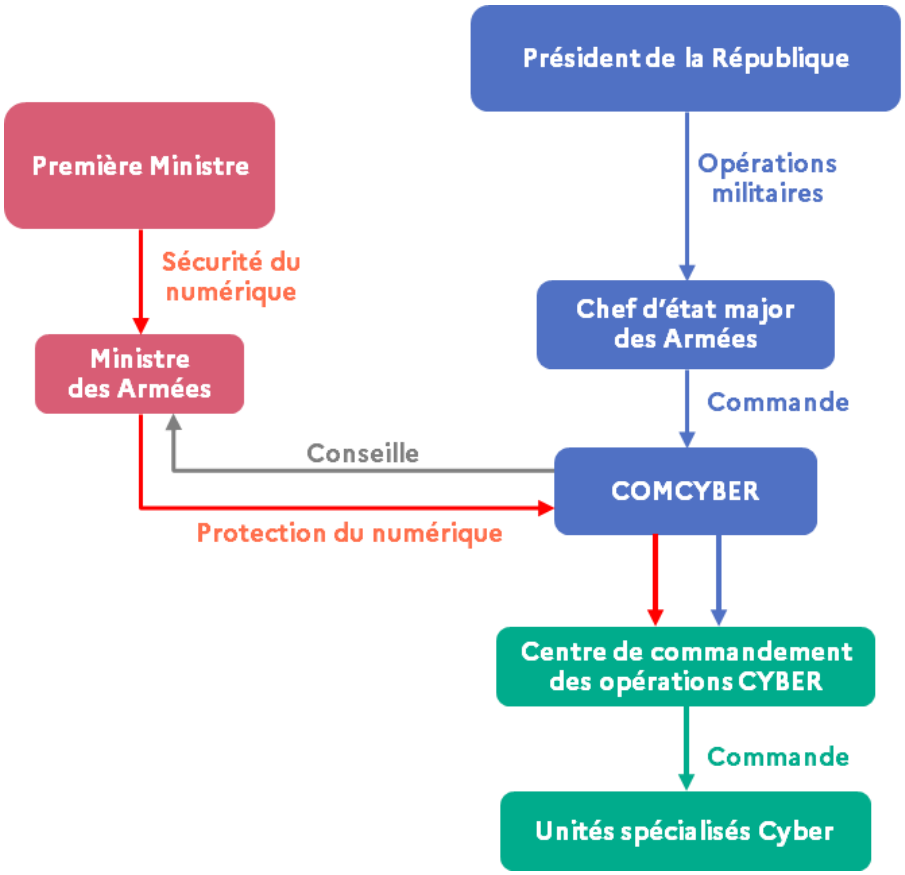
En résumé :

- L'attaque cyber contre l'Estonie en 2007 (officiellement attribuée à la Russie) fait prendre conscience à la France de la nécessité de créer une agence nationale destinée à la protection du son cyberespace : l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).
- Dès 2011, **un officier général est nommé responsable de la conduite de la cyberdéfense** et conseiller du ministre. Il prend le titre d'OG CYBER.
- Une décennie d'attaques majeures contre la France (cyberattaques comme celle contre TV5 Monde mais également les attaques terroristes notamment en 2015) entrainent des réactions politiques exceptionnelles fortes qui permettent une structuration complète de l'action de l'état dans le cyberespace. La revue stratégique de cyberdéfense de 2018 formalise **la création de quatre chaines opérationnelles de défense :**



Pour le ministère des Armées, **un commandement de la cyberdéfense (COMCYBER)** militaire est créé dès 2017, placé sous les ordres de l'OG CYBER (devenant OG COMCYBER) et sous l'autorité directe du chef d'état-major des Armées (CEMA). La structure du COMCYBER continue encore aujourd'hui d'évoluer et de s'étoffer pour faire face aux différentes menaces et conduire avec efficacité des opérations militaires dans le cyberespace.

Représentation graphique synthétique des deux chaines opérationnelles « Sécurité du numérique » et « Opérations militaires »



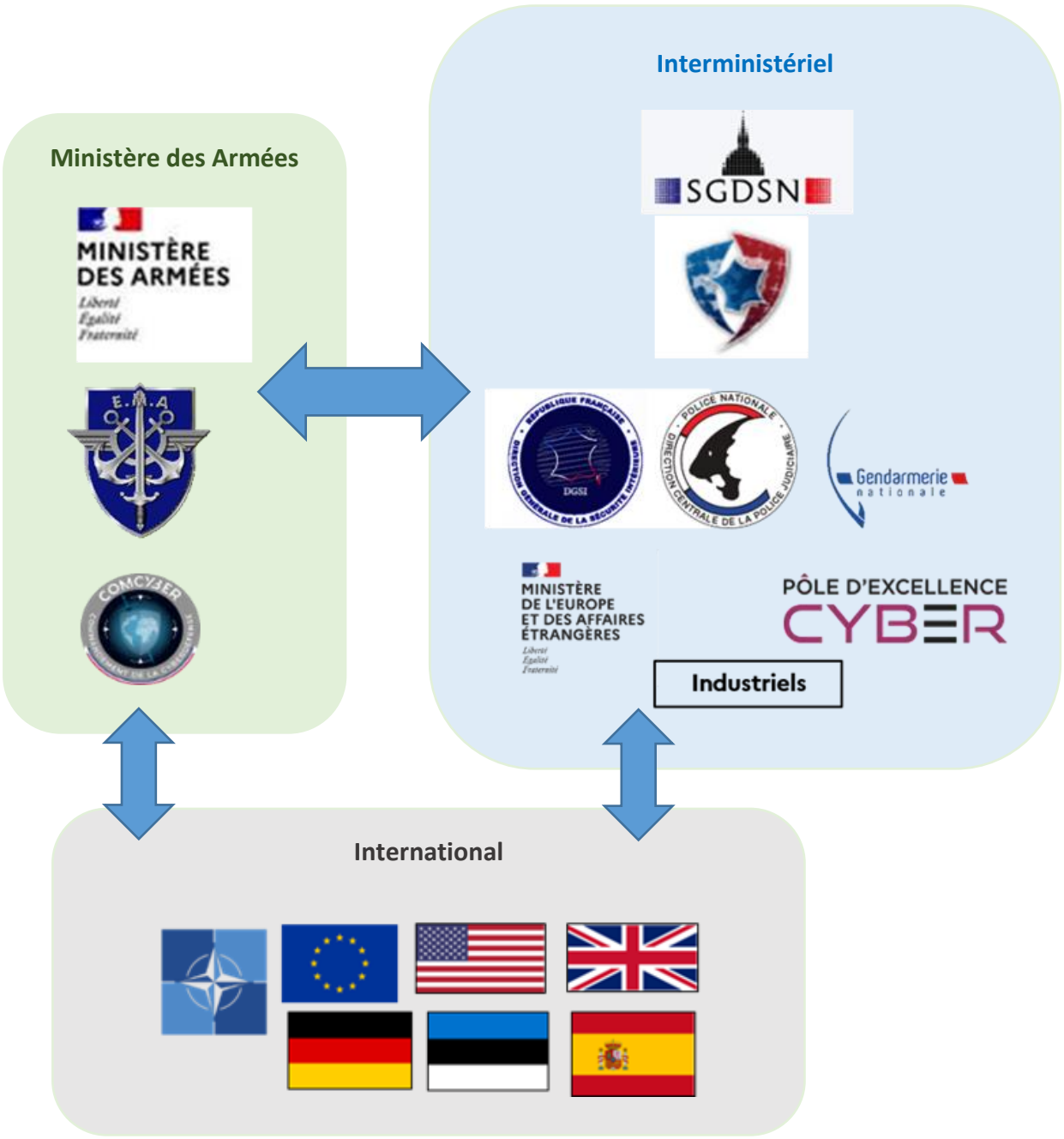
Dans le domaine de la cyberdéfense, même si la part du secret est toujours prédominante et importante, il est **nécessaire de mettre en œuvre des coopérations avec des alliés et partenaires** afin de pouvoir, a minima, échanger des renseignements sur l'état de la menace ou sur les actions conduites. **La France est un acteur majeur de la cyberdéfense et un partenaire important de confiance d'autres grandes nations** (accords bilatéraux) **et d'organisations internationales** (Organisation du Traité de l'Atlantique Nord –OTAN) ou l'Union Européenne –UE). Au niveau national, les différents services étatiques se coordonnent et coopèrent de manière concertée.

En 2020, l'institut des hautes études de la défense nationale (IHEDN) et l'institut des hautes études du ministère de l'Intérieur (IHEMI) ont établi une cartographie très précise des acteurs formant la communauté étatique cyber française et européenne. Ce document dense ne peut être reproduit dans la fiche en raison de son manque de lisibilité sur un petit format mais est librement consultable à l'adresse suivante :

https://www.ihemi.fr/articles/organisation-france-europe-cybersecurite-cyberdefense-V2

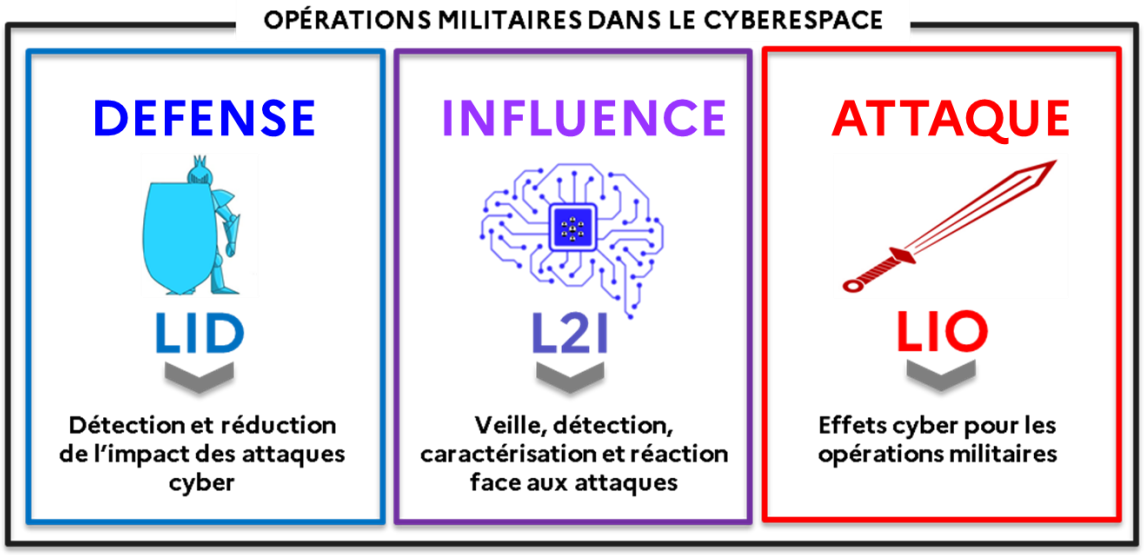
De manière plus simplifiée, le schéma ci-dessous présente un état très synthétique des relations et de l'environnement du COMCYBER en interministériel et à l'international :

L'environnement du COMCYBER



LES OPÉRATIONS MILITAIRES DANS LE CYBERESPACE

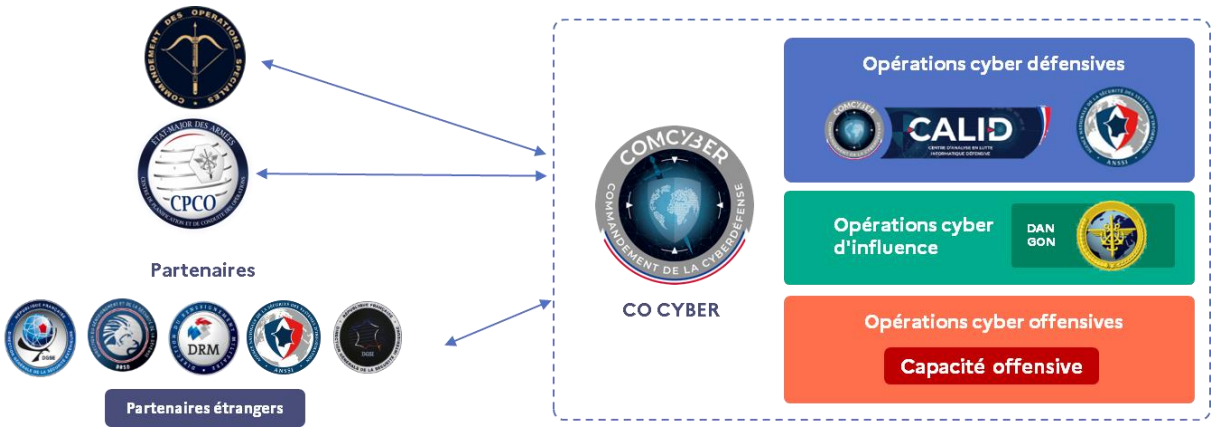
Pour remplir sa mission et couvrir l'ensemble du spectre des menaces dans le cyberespace**, l'action militaire française est organisée en trois domaines de lutte informatique** avec chacun ses spécificités techniques et faisant appel à des compétences variées :



Pour mener à bien les opérations militaires dans le cyberespace, le COMCYBER dispose de ressources internes (état-major et effecteurs). Il s'appuie également sur les armées, directions et services du MINARM et coordonne ses actions sous l'autorité du CEMA. Le COMCYBER coopère aussi avec tout un écosystème interministériel et international.

Le schéma ci-dessous illustre bien l'environnement du COMCYBER dans les différents domaines de lutte qui sont détaillés et explicités *infra* dans ce paragraphe.

Les partenaires du COMCYBER dans les domaines de lutte informatique



Il est important de souligner que le MINARM a fait preuve d'une grande transparence en publiant sur son site internet des éléments de doctrine publique relatifs aux trois domaines de lutte et accessibles par le lien suivant :

https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees

Ces documents très complets et clairs permettent de bien saisir les missions et enjeux dans chacun des domaines. Ils sont facilement exploitables par les enseignants et sont complétés par un guide relatif au droit international applicable aux opérations militaires dans le cyberespace.

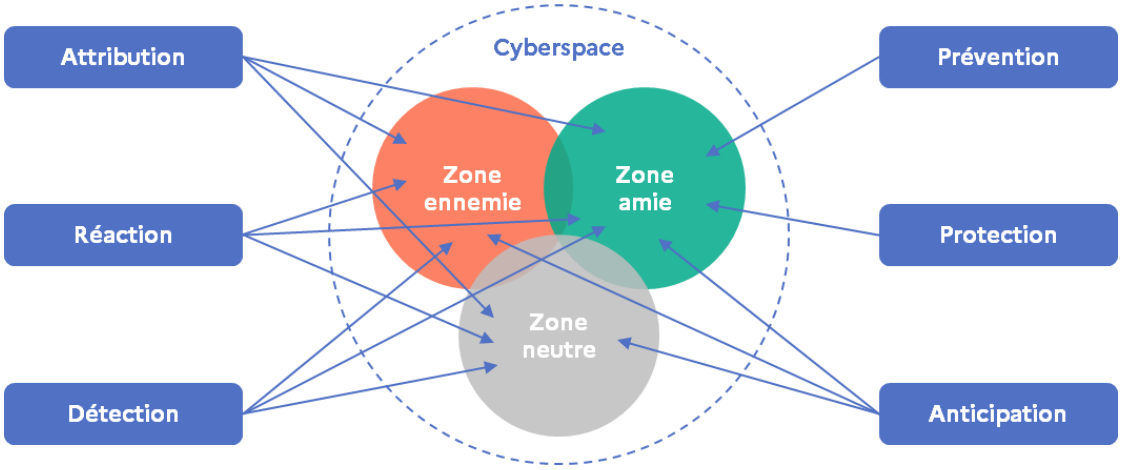
3.1. La lutte informatique défensive (LID)

La protection des réseaux informatiques et des systèmes d'information constitue le premier rempart pour empêcher une attaque informatique. Si ce premier rempart est indispensable, la dynamique de numérisation des systèmes qui soutiennent les activités du ministère, y compris au profit de son engagement opérationnel via ses systèmes de commandement et ses systèmes d'armes, offre de nouvelles opportunités aux attaquants. Elle impose donc de développer de nouveaux modes de défense, adaptés à ces nouvelles menaces.

Pour atténuer leur vulnérabilité, les systèmes militaires français doivent offrir et garantir le meilleur niveau de « défendabilité » possible. Il s'agit, d'une part, de s'assurer de la bonne prise en compte du risque d'attaque cyber et des potentielles conséquences sur les organisations ou individus visés et, d'autre part, d'être en mesure d'adapter notre capacité d'action et de réaction à une attaque cyber, en fonction du contexte opérationnel ou de la réalité de la menace.

Les actions de prévention et de protection concernent les systèmes informatiques du ministère des Armées (zone amie). Les missions d'anticipation, de détection et de réaction s'intéressent aux systèmes informatiques appartenant aux autres catégories d'acteurs (zones neutre et ennemi).

Les différentes zones du cyberespace et les actions du COMCYBER sur ces zones



La LID regroupe l'ensemble des actions, techniques et non techniques, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle, en vue de préserver la liberté d'action.

La LID couvre principalement trois de ces missions : **anticiper, détecter et réagir** et complète les missions : **prévenir, protéger et attribuer**. Elle contribue ainsi à la résilience des armées et plus globalement à l'élaboration des stratégies de réponse aux niveaux ministériel et interministériel.

Au sein du ministère des Armées, les opérations de LID sont planifiées et conduites par le COMCYBER, en coordination avec l'ANSSI, les services de renseignement, et éventuellement d'autres partenaires (nationaux ou internationaux). Dans un souci de cohérence et d'efficience, la chaîne de commandement de cette cyberdéfense est dite unifiée, centralisée et spécialisée pour tout le ministère.

C'est-à-dire qu'elle est **pilotée et coordonnée par le COMCYBER** et que, **composée d'experts de la cyberdéfense**, elle doit en outre **favoriser les synergies entre les différentes organisations de LID tout en permettant de disposer d'une vision globale de la situation cyber.** La mobilisation rapide des moyens et des compétences disponibles passe par le partage des procédures et des outils de gestion de crise. De même, une cyberdéfense efficace passe par une plus grande intégration avec les partenaires nationaux et une forte coordination avec les partenaires internationaux et les industriels.

Ces interactions imposent de renforcer l'interopérabilité des organisations et des capacités à tous les niveaux, techniques et décisionnels.

Le cyberespace est un milieu de confrontation pour les Etats ou les organisations non gouvernementales dans lequel le risque d'attaque est considéré comme permanent, y compris en temps de paix. La tension générée par ces attaques cyber, cycliques ou soudaines, de gravités variables, impose l'adoption d'une vigilance de tous les instants, qui s'incarne à travers la posture permanente de cyberdéfense (PPC) pour le ministère des Armées. La PPC est constituée de l'ensemble des dispositions adoptées pour assurer en permanence (24h/7j) la défense des systèmes informatiques du ministère.

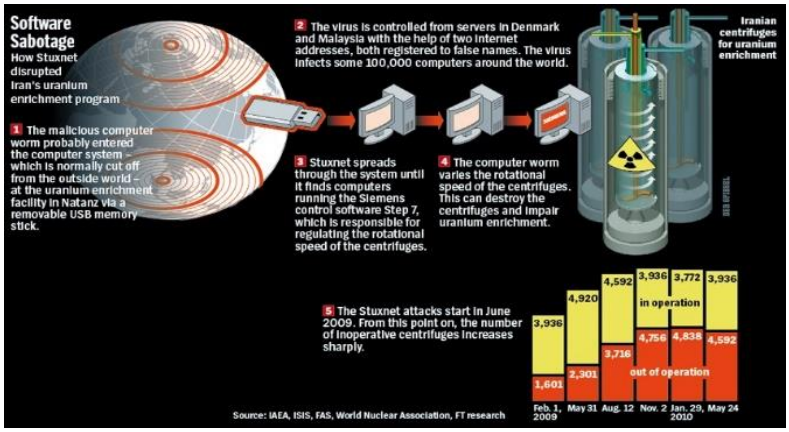
3.2. La lutte informatique offensive (LIO)

La lutte informatique offensive à des fins militaires (LIO) recouvre l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels. L'arme cyber vise, **dans le strict respect des règles internationales**, à **produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données.**

Lorsqu'elle est combinée aux modes d'action conventionnels, la LIO prend sa pleine dimension de potentiel **multiplicateur d'effets** - amplifier, améliorer ou compléter. Elle tire notamment partie de la mise en réseau croissante de l'ensemble des systèmes militaires, ainsi que de leurs interconnexions avec l'Internet.

Face à un adversaire, la LIO propose **des modes d'actions discrets et efficaces contre les systèmes numérisés, capables de se substituer à d'autres modes d'action, de les préparer ou les compléter**. La LIO permet de **tirer parti de vulnérabilités dans les systèmes numériques adverses** durant toutes les phases d'une crise : renseignement, prévention, gestion ou stabilisation.

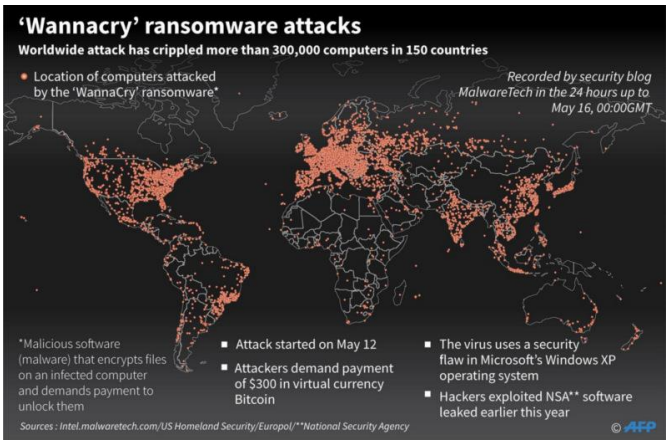
Les cibles visées peuvent être exposées sur Internet, isolées, ou partie intégrante d'un système d'armes plus global. La LIO contribue à la sécurisation, voire à la préservation des moyens numérisés utilisés par nos forces déployées. Les actions de LIO ne sont pas nécessairement menées au contact physique de l'adversaire. **La LIO peut aussi venir en appui de la lutte informatique défensive lorsque l'attaque informatique vise exclusivement les capacités opérationnelles des armées ou les chaînes de commandement de la défense** en participant à la caractérisation d'une attaque, en faisant cesser une agression cyber sur nos systèmes, conformément à l'article L. 2321-2 du code de la défense[2] ou en imposant une diversion de ses efforts vers des cibles inutiles.



La LIO repose sur des savoir-faire sensibles et constitue un des attributs d'une défense souveraine. Ces deux dimensions imposent un contrôle stratégique des opérations de LIO, de leur planification jusqu'à leur mise en œuvre. **Sous l'autorité du Président de la République et aux ordres du chef d'état-major des armées, le COMCYBER a la responsabilité de planifier et de coordonner des opérations LIO au profit des Armées.**

Les opérations de LIO sont **conduites par des unités spécialisées,** dont l'expertise garantit l'analyse des risques et la maîtrise des effets, collatéraux voire fratricides, induits par la complexité du domaine cyber et des interconnexions. L'action de ces unités spécialisées est pleinement intégrée à la manœuvre des armées, directement sur le terrain ou à distance.

Aux ordres de l'officier général COMCYBER, **l'emploi de la LIO exige une maîtrise des risques politique, juridique et militaire dans toutes les phases de l'opération**. Comme toute opération militaire, la LIO implique une acceptation du risque par l'échelon décisionnel, déterminée par les principes du *jus in bello* (proportionnalité, distinction, discrimination, …), le rapport coût/efficacité, la situation opérationnelle et le contexte politique général.



Pour en préserver l'efficacité et maîtriser les risques de détournement, l'ensemble des opérations de LIO menées par les forces armées demeure de nature secrète, mais les autorités politiques et militaires peuvent, selon les circonstances, les assumer publiquement voire les revendiquer. Cette posture est de la responsabilité de l'autorité politique. La décision de rendre publique une action de LIO doit, in fine, être mise en balance avec le risque que représente la vulnérabilité inhérente à la forte numérisation de nos intérêts nationaux.

La LIO est soumise, comme toute autre arme ou méthode de guerre, aux principes et règles du droit international, notamment le droit international humanitaire, ainsi qu'aux lois et règlements nationaux. Elle n'est donc utilisée que dans le respect de règles opérationnelles d'engagement très restrictives.

La France recherche l'adoption de règles de comportement responsable et de codes internationaux de bonne conduite pour prévenir les situations de conflit dans le cyberespace, y garantir la stabilité stratégique et, le cas échéant, à terme, servir de référence à d'éventuels développements du droit international.

[2] Article 21 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

Au niveau européen, la France joue un rôle moteur dans la promotion d'une culture militaire cyber partagée et ambitionne de développer les moyens d'interopérabilité opérationnelle avec nos principaux partenaires européens.

3.3. La lutte informatique d'influence (L2I)

La guerre de l'information est partie intégrante de toute stratégie militaire : sans capacité à convaincre et à contrer l'influence adverse, tout engagement militaire est voué à l'échec. L'avènement des réseaux sociaux a renforcé ce postulat, accélérant considérablement la circulation d'informations vraies ou fausses et augmentant dans le même temps le volume, la portée et la résonance de ces informations. Des agresseurs potentiels disposent ainsi de la capacité à mobiliser rapidement la violence, en parole et en actes, et à fragiliser la légitimité des différents acteurs du règlement d'une crise. La guerre de l'information s'est déployée dans le cyberespace, y trouvant un terreau particulièrement fertile.

Engagées sous l'autorité du Président de la République sur les théâtres d'opération et dans des missions de souveraineté et de protection du territoire national**, les armées françaises font l'objet d'attaques informationnelles dans le cyberespace, orchestrées par des groupes ou des États hostiles à leur action**. Ainsi que le constate le Concept d'emploi des forces de décembre 2020, elles doivent être prêtes à combattre et à conquérir la supériorité dans ce champ de confrontation. Pour cela, les armées disposent désormais d'une doctrine de lutte informatique d'influence (L2I) qui organise et structure ce combat, offre un cadre et des outils pour l'action, ainsi que des clefs pour l'interopérabilité avec d'autres partenaires nationaux ou étrangers.

Les opérations de L2I se déroulent dans un cadre strictement limité aux opérations militaires à l'extérieur du territoire national.

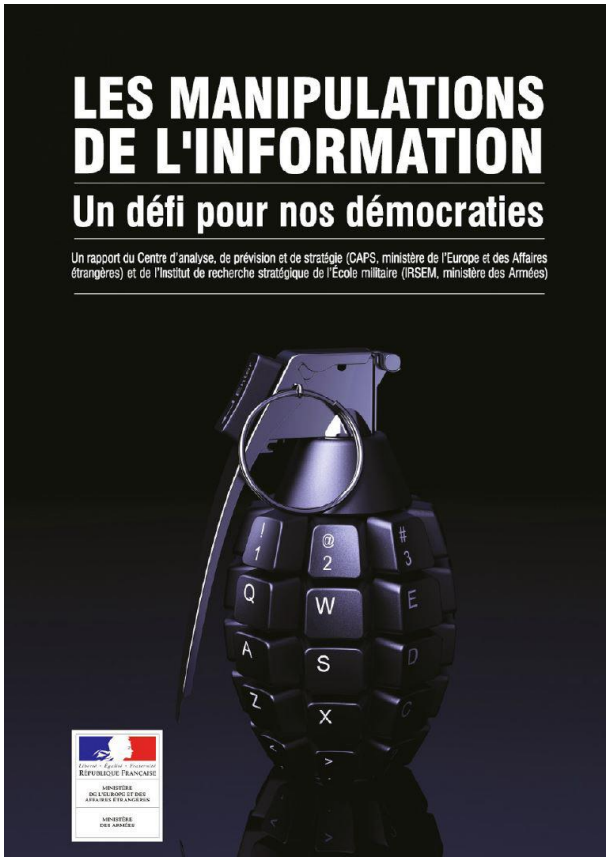
L'actualité récente des opérations montre qu'un certain nombre de nos compétiteurs et adversaires actuels ou potentiels ont pleinement intégré le besoin de maîtriser la couche informationnelle du cyberespace, partie émergée de cet espace incluant notamment le Web et les réseaux sociaux.

Exemple de fabrication d'une désinformation orchestrée par la société militaire privée Wagner (Russie), avec l'organisation d'une manifestation artificielle, faite par des acteurs rémunérés et habilement insérés dans un rassemblement quotidien anodin (marché) dans le but d'amplifier l'image, qui sera ensuite très largement diffusée sur les réseaux sociaux dans le cadre d'une attaque informationnelle contre la France et l'ONU.

Les manipulations de l'information s'inscrivent typiquement dans le cadre de **stratégies hybrides**[3] et donnent lieu **à une véritable guerre de l'information**. Elles visent directement les capacités des armées françaises (ex : démoralisation des troupes), ou la perturbation de la conduite de l'opération, notamment par la propagation de fausses informations (*fake news*). Elles complètent des actions menées dans les champs militaire, économique et diplomatique, dans tout le spectre de la conflictualité du temps de paix au conflit de haute intensité.

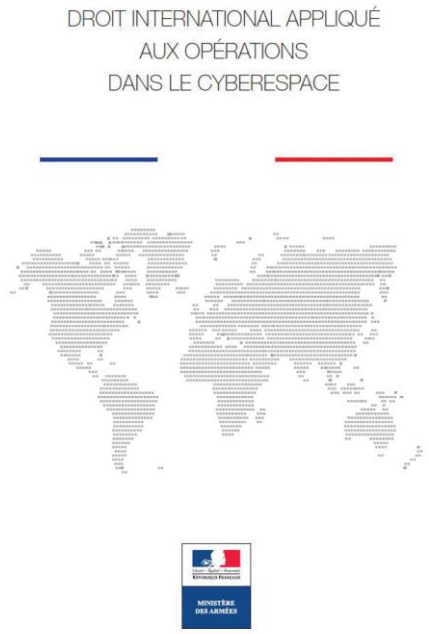
L'extension du combat de l'information vers le cyberespace est un générateur d'instabilité dans l'environnement des opérations militaires. Elle fait peser au quotidien des risques sur les forces armées et peut compromettre leurs chances de succès. Il importe donc de déjouer les attaques fomentées sur les réseaux sociaux, de tarir les recrutements des groupes armés terroristes sur les théâtres d'opérations réalisées par leur biais et de promouvoir la crédibilité et la légitimité des forces engagées en opération afin de conserver le soutien des opinions publiques.

Amplifiant certaines menaces, le cyberespace offre de nouvelles opportunités pour produire des effets à la fois dans les environnements informationnels et physiques, entraver l'action adverse et collecter des informations dans le cadre des opérations militaires. La conquête, puis la maîtrise de la supériorité dans le champ informationnel sont devenues des conditions de la supériorité opérationnelle.



Comme l'ensemble des opérations menées par les armées françaises, **la L2I est soumise aux principes et règles du droit international, ainsi qu'aux normes du droit interne.** Sous l'autorité du Président de la République, et conformément aux engagements pris par la France, **les opérations militaires de L2I sont menées dans le strict respect du droit, national et international**. Le développement des capacités afférentes, outils de veille et d'action numérique et ressources humaines spécialisées, est prévu par la loi de programmation militaire que ce ministère s'attache à mettre en œuvre intégralement. **La France s'attache à promouvoir l'action de ses forces armées et à contrer le narratif propagandiste.**

[3] Stratégies combinant une palette d'outils hors du champ militaire pour affaiblir un adversaire sans passer le seuil du conflit armé. La stratégie hybride peut se définir comme la « stratégie d'un acteur, étatique ou non, visant à contourner ou à affaiblir la puissance, l'influence, la légitimité et la volonté adverse tout en affirmant sa propre légitimité, en mettant en œuvre une combinaison intégrée de modes d'action militaires et non militaires, directs et indirects, licites ou illicites, souvent subversifs, ambigus et difficilement attribuables, visant à désorganiser et à paralyser et pouvant être engagés sous un seuil estimé de riposte ou de conflit ouvert et dans le cadre d'une possible gestion d'escalade ».



Manuel sur l'application du droit international aux opérations dans le cyberespace, publié en octobre 2019

Pour chaque opération, des règles opérationnelles d'engagement (ROE) sont élaborées afin de définir les circonstances et les conditions dans lesquelles les opérations de L2I peuvent être mises en œuvre, compte tenu des contraintes et des finalités politiques, opérationnelles et juridiques auxquelles elles doivent répondre.

Face à la manipulation de l'information et à la propagande terroriste sur les réseaux sociaux, les opérations militaires de L2I s'inscrivent dans l'ensemble de l'action publique**. Contrer une attaque informationnelle nécessite à la fois de pouvoir la détecter, la caractériser et, pour la contrer, de coordonner si nécessaire les actions militaire, diplomatique et intérieure, avec l'apport des entreprises spécialisées dans le numérique.**

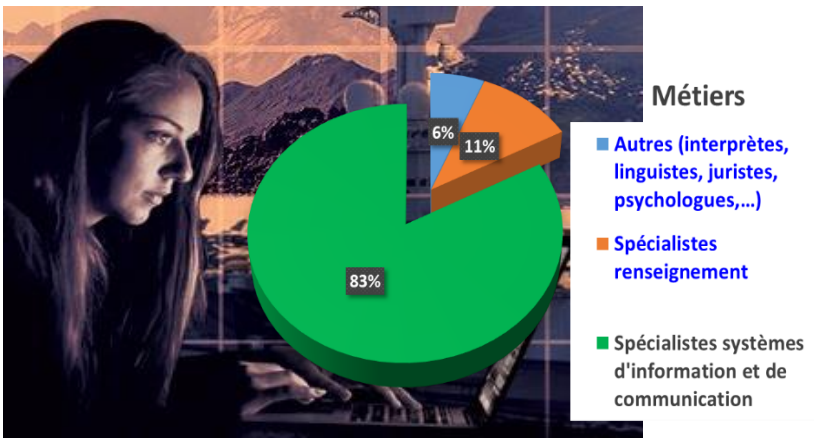
Fidèle à ses engagements internationaux, la France promeut et soutient les initiatives de l'UE et de l'OTAN pour lutter contre les manipulations de l'information. Fortes de leur doctrine de Lutte informatique d'influence, les armées seront des contributrices déterminées à l'action collective dans ce domaine.

LES CYBERCOMBATTANTS

Les ressources humaines dans le domaine de la cyberdéfense, et plus globalement dans le secteur très concurrentiel de la cybersécurité, constitue un enjeu majeur qu'il ne faut absolument pas négliger. Afin de pouvoir agir efficacement dans le cyberespace, il est nécessaire de disposer de personnels compétents qu'il faut identifier, recruter, éventuellement former, mais dans tous les cas maintenir à niveau voire faire progresser techniquement et professionnellement avec l'objectif de les conserver sur le long terme. Il s'agit donc d'un véritable défi pour le COMCYBER qui se dote de moyens ambitieux pour y parvenir.

4.1. Des métiers aussi divers que passionnants

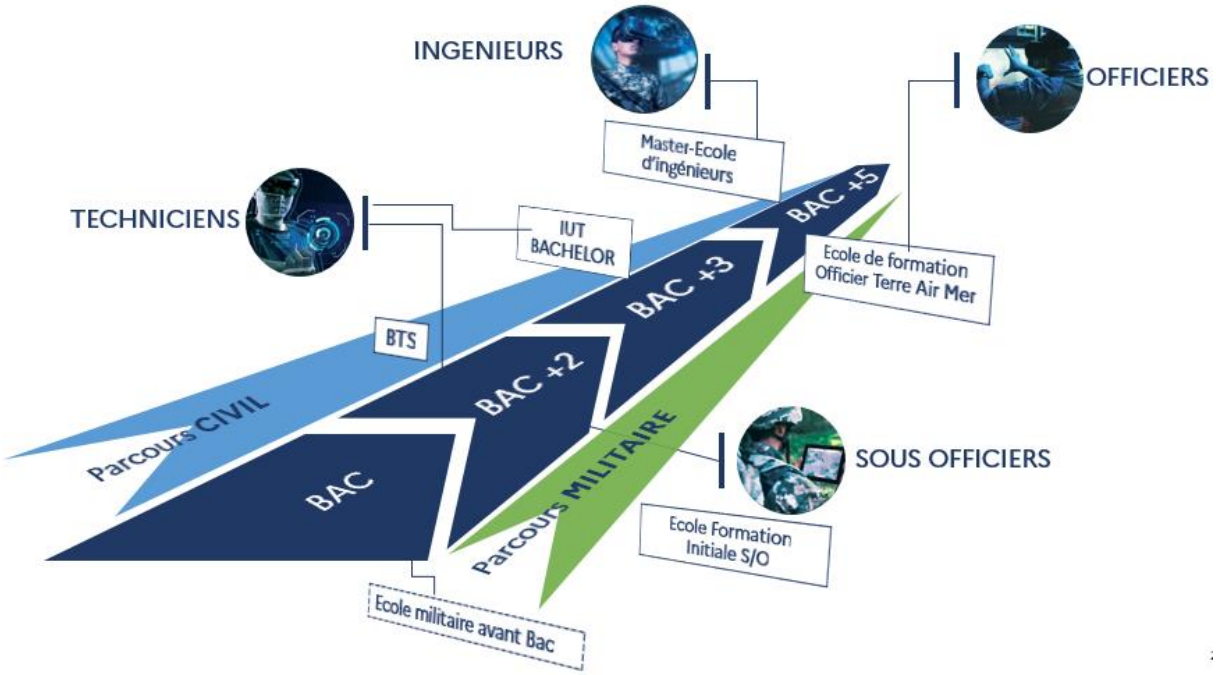
La Loi de Programmation Militaire 2019-2025 consacre à la cyberdéfense des moyens à la hauteur des défis identifiés. L'actualisation de la revue stratégique de 2021 a encore renforcé la priorité accordée à ces moyens. Ainsi, le ministère des armées a augmenté de 770 son objectif initial de recrutement de 1100 cyber combattants supplémentaires, pour porter l'effectif de cybercombattants à **5000 femmes et hommes** d'ici 2025.



Cet effectif sera constitué de 77 % de militaires et **23 % de civils** (actuellement 13 % de cybercombattant**e**s), et plus d'un cybercombattant sur 6 n'est pas un « informaticien ». Le COMCYBER a aussi besoin de juristes, spécialistes des relations internationales, de linguistes et de profils diversifiés dans le domaine du renseignement.

Tous les ans, le Ministère des Armées attribue des Bourses (allocation financière spécifique de formation) aux étudiants s'engageant à servir en qualité de militaire après l'obtention d'un diplôme ou la validation d'une formation intéressant l'armée. Le montant de la bourse et la durée d'engagement sont variables selon le diplôme. Montant pouvant aller de 3 000 € à 15 000 € pour un engagement de 2 à 4 ans[4].

Des parcours de carrières variés



Une attention particulière est également portée sur la montée en puissance de la réserve cyber, lien privilégié entre la nation, les citoyens et les armées. Le double objectif du COMCYBER est de recruter et d'employer ses réservistes opérationnels (ROPS) (statut militaire) et les réservistes citoyens (statut bénévole), mais aussi de les faire participer les ROPS aux entrainements LID du COMCYBER. Cette participation peut s'effectuer sur des formations, mais aussi lors d'exercices d'entrainement majeurs et même sur des missions opérationnelles où les réservistes travaillent aux côtés des militaires d'active et les renforcent efficacement.

4.2. Brain games, serious games et wargames : la « ludification » au service de l'anticipation

Dans un domaine technique en constante évolution, la formation, la montée en compétence et la consolidation des savoir-faire constituent des enjeux importants pour le COMCYBER qui a des ambitions fortes dans ce domaine. Des formations et entraînements sont mis en œuvre notamment par le Centre de Cyber de Préparation Opérationnelle (C2PO) avec des degrés de technicité et de complexité variables selon les besoins et les publics ciblés. La qualité d'enseignement du C2PO est largement reconnue et le centre continue sa montée en puissance progressive.

Le COMCYBER participe également à des exercices d'envergure et de dimension internationale comme :

[4] https://www.welcometothejungle.com/fr/companies/commandement-de-la-cyberdefense-comcyber et https://www.stages.defense.gouv.fr

- **DEFNET :**

Chaque année, 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 opérations et sur le territoire national, dans un scénario fictif.

Cet exercice de type « Capture the flag » est piloté à Rennes depuis le CALID et les équipes chargées de l'organisation sont déployées sur plusieurs sites militaires en France (Paris, Satory, Rennes, Brest, Mont-de-Marsan, Istres, Toulon et Hyères). Les réservistes opérationnels de cyberdéfense viennent renforcer les effectifs et s'entraîner aux procédures militaires de gestion de crise. Il est également proposé aux élèves du Secondaire et de BTS en Ile de France (https://www.defense.gouv.fr/sites/default/files/operations/Passe%20ton%20hack%20d%27abord%20-%20Reglement%20-%202601.pdf)

Le maintien d'un haut niveau d'expertise exige également un renforcement de la coopération entre acteurs militaires, publics et privés. DEFNET intègre donc, à plusieurs niveaux, les industriels et principaux équipementiers, signataires de la convention relative à la cybersécurité, pour la défense des systèmes d'armes en service.

- **LOCKED SHIELDS :**

Ou l'exercice LOCKED SHIELDS, qui est un exercice international d'entrainement des chaînes de lutte informatique défensive sous la direction du NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) de Tallinn. Pour la France, l'édition 2022 a vu la mise en œuvre d'une équipe regroupant des spécialistes issus du MINARM et de l'ANSSI, mais également du CERT UE afin de créer une « joint Blue Team ». Bien que le cœur de cible soit le volet technique, cet exercice offre l'opportunité de stimuler les autres volets juridique, stratégique et de communication en les faisant coopérer autour d'une animation de la chaîne de commandement allant du stratégique au tactique.

FOND DOCUMENTAIRE

5.1. Références textuelles

- Revue stratégique de cyberdéfense (2018)

  https://www.leslivresblancs.fr/livre/informatique-et-logiciels/cybersecurite/revue-strategique-de-cyberdefense

- L'Appel de Paris pour la confiance et la sécurité dans le cyberespace (2018)

  https://pariscall.international/fr/

- Droit international appliqué aux opérations dans le cyberespace (2019)

  https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees

- Doctrines nationales d'attribution et de réponse (2020)

  https://www.senat.fr/rap/r19-007-1/r19-007-17.html

- Déclaration de M. Emmanuel Macron, président de la République, sur les cyberattaques dans les hôpitaux et la stratégie nationale pour la cybersécurité, à Paris le 18 février 2021 (Nouvel Elan Cyber)

  https://www.vie-publique.fr/discours/278659-emmanuel-macron-18022021-cybersecurite

- Instruction n°101000 relative à la politique de lutte informatique et défensive du ministère des Armées (2019)

  https://www.legifrance.gouv.fr/circulaire/id/44356

- Politique ministérielle de lutte informative défensive (2019)

  https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees

- Eléments publics de doctrine militaire de lutte informatique offensive (2019)

  https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees

- Eléments publics de doctrine militaire de lutte informatique d'influence (2021)

  https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees

- Déclaration de M. Emmanuel Macron, président de la République, sur la politique de défense de la France, à Mont-de-Marsan le 20 janvier 2023

  https://www.vie-publique.fr/discours/287928-emmanuel-macron-20012023-politique-de-defense

GLOSSAIRE DES TERMES EMPLOYÉS ET DES ACRONYMES UTILES À CONNAÎTRE

ANSSI	Agence nationale de sécurité des systèmes d'information
CALID	Centre d'analyse en lutte informatique défensive
CEMA	Chef d'état-major des armées
CERT	Equipe cyber d'intervention rapide *(Computer Emergency Response Team)*
CIAE	Centre interarmées des actions sur l'environnement
CO CYBER	Centre opérationnel de la cyberdéfense
COMCYBER	Commandement de la cyberdéfense
COMCYBERGEND	Commandement de la gendarmerie dans le cyberespace
CPCO	Centre de planification et de conduite des opérations
C2PO	Centre cyber de la préparation opérationnelle
DGA	Délégué général pour l'armement
DGSE	Direction générale de la sécurité extérieure
DRM	Direction du renseignement militaire
DRSD	Direction du renseignement et de la sécurité de la défense
EMA	État-major des armées
GCA	Groupement de la cyberdéfense des armées
GIC	Groupe d'intervention cyber
LID	Lutte informatique défensive
L2I	Lutte informatique d'influence
LIO	Lutte informatique offensive
LPM	Loi de programmation militaire
MEAE	Ministère de l'Europe et des Affaires étrangères
MINARM	Ministère des Armées
OCYBER	Officier de cyberdéfense militaire
OG COMCYBER	Officier général « commandant de la cyberdéfense »
OIV	Organisme d'importance vitale
PPC	Posture permanente de cyberdéfense
ROE	Règles d'engagement *(Rules of engagement)*
ROPS	Réservistes opérationnels
SECNUM	Sécurité numérique
SGA	Secrétaire général pour l'administration
SGDSN	Secrétariat général de la défense et de la sécurité nationale