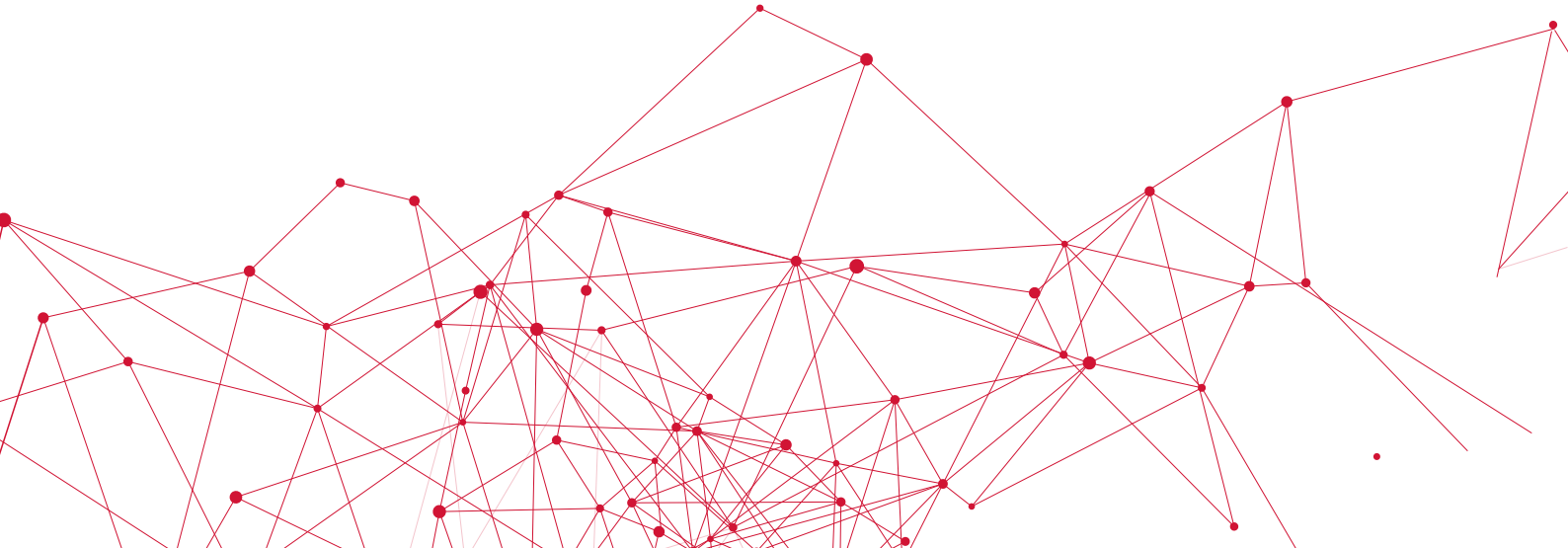
Éléments publics de doctrine militaire de lutte informatique offensive

COMCYBER
COMMANDEMENT DE LA CYBERDÉFENSE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

SOMMAIRE



PRÉAMBULE

Puissance militaire nucléaire, conventionnelle et cyber, membre permanent du Conseil de sécurité de l'Organisation des Nations unies, de l'Organisation du traité de l'Atlantique nord et de l'Union européenne, la France assume, sous l'autorité du Président de la République, ses engagements sur la scène internationale. Dans un environnement géopolitique en proie aux crises, à la déstabilisation, à la menace terroriste et aux guerres conventionnelles et hybrides, le ministère des Armées contribue à garantir, en toutes circonstances, en temps de paix ou de guerre, la souveraineté nationale et l'autonomie de décision de la France, sur le territoire national comme sur tous les théâtres extérieurs où sont déployées nos armées.

Les cyberattaques contre l'Estonie en 2007, contre les réseaux électriques de l'Ukraine, contre TV5 Monde en 2015, le rançongiciel Wannacry au printemps 2017 ou encore l'attaque NotPetya en juin 2017, illustrent les champs d'actions possibles pour des attaquants dont les quatre objectifs majeurs sont l'espionnage, les trafics illicites, la déstabilisation et le sabotage.

La plupart des luttes de pouvoir, des crises et des conflits contemporains connaissent un développement dans l'espace numérique. Les armées doivent désormais, systématiquement, regarder le combat cybernétique comme un mode d'action à part entière dont les effets se combinent aux autres dans une manœuvre globale.

Véritable rupture en termes de technologie et d'emploi de la force, l'arme cyber est amenée à bouleverser les modalités de la guerre sans en renouveler profondément les principes. Multiplicité d'acteurs étatiques, masqués ou non, organisations terroristes, frontières gommées, perceptions troublées, repères faussés, propagation rapide, droit international non respecté, code de conduite bafoué : tels sont les risques du cyberespace. Une zone grise, un brouillard, dont les effets, eux, sont bien réels, parfois dévastateurs. Le combat dans le cyberespace est de nature asymétrique, hybride, parfois invisible et en apparence indolore. Pourtant, l'emploi de l'arme cyber est susceptible de porter gravement atteinte aux capacités et aux intérêts souverains des États.

La revue stratégique de cyberdéfense, publiée en février 2018, a confirmé la pertinence de notre modèle d'organisation et de gouvernance qui sépare les missions et capacités offensives des missions et capacités défensives. Elle a proposé une stratégie à part entière dans ce domaine en structurant l'organisation de la cyberdéfense autour d'un centre de coordination interministériel des crises cyber animé par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) sous l'autorité du Premier ministre et de quatre chaînes opérationnelles distinctes. En complément des chaînes « protection », « renseignement » et « investigation judiciaire », la chaîne « action militaire » a notamment recours à la lutte informatique offensive (LIO).

La France consolide ainsi un modèle rénové de cyberdéfense, dont la création du commandement de la cyberdéfense (COMCYBER) en mai 2017[1] avait constitué une des étapes fondatrices au sein du ministère des Armées. Le COMCYBER a la responsabilité de la cyberdéfense militaire, qui recouvre l'ensemble des actions défensives et offensives conduites dans le cyberespace pour garantir le bon fonctionnement du ministère et l'efficacité des forces armées, dans la préparation, la planification et la conduite des opérations militaires.

Désormais, le ministère des Armées dispose de capacités et d'une doctrine d'emploi qui couvrent les actions cyber offensives dédiées à l'engagement des forces armées.

1 Décret n° 2017-743 du 4 mai 2017 relatif aux attributions du chef d'état-major des armées et l'arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées.

AGIR DANS LE CYBERESPACE : la lutte informatique offensive à des fins militaires, une arme de supériorité opérationnelle

La capacité à conduire des opérations militaires défensives et offensives dans le cyberespace contribue à garantir la souveraineté nationale. Elle participe à l'obtention d'avantages opérationnels sur les théâtres d'engagement de nos forces armées, mais aussi à la défense des systèmes d'information des armées. Ainsi, les forces armées se dotent de l'ensemble du spectre des moyens de lutte informatique désormais nécessaires à la conduite des opérations : défensif, offensif et contre les manipulations de l'information nuisibles à nos opérations militaires.

Sous l'autorité du chef d'état-major des armées, le COMCYBER est l'autorité d'emploi de la capacité militaire cyber offensive, partie intégrante de la chaîne opérationnelle des armées, en parfaite cohérence avec leur organisation et leur structure opérationnelle.

1) LA LUTTE INFORMATIQUE OFFENSIVE À DES FINS MILITAIRES : UNE CAPACITÉ AGILE ET NOVATRICE

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[2], à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données.

La variété des effets de la LIO et des modes d'action correspondant tient à la nature du cyberespace, nouveau champ de confrontation. Celui-ci repose sur une structure en trois couches :

- une couche physique, constituée des équipements des systèmes informatiques et de leurs réseaux ayant une existence matérielle et, pour certains d'entre eux, une existence électromagnétique (ordinateurs, processeurs, câbles, fibres, émetteurs, récepteurs, liens satellitaires, routeurs etc.) ;

- une couche logique, constituée de l'ensemble des données numériques, des processus et outils de gestion et d'administration de ces données, ainsi que de leurs flux d'échanges (fichiers, sites, adresses, codes de connexion, protocoles, logiciels, applications etc.), implantés dans les matériels pour leur permettre de rendre les services attendus ;

- une couche sémantique et sociale, constituée par les informations qui circulent dans le cyberespace et par les personnes qui peuvent disposer de multiples identités numériques ou « avatars » (pseudonymes, adresses de messagerie, adresses IP, blogs etc.).

L'interdépendance de ces trois couches renforce les opportunités d'actions de la LIO et donc de déstabilisation de l'adversaire.

2 Comme le précise la revue stratégique de cyberdéfense, ces règles définissent notamment les conditions du déclenchement ou de l'adoption de mesures de rétorsion, de contre-mesures ou même du recours à la force en cas d'agression armée justifiant la légitime défense.

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.

L'emploi de la LIO s'inscrit dans une temporalité qui lui est propre. Si ses effets peuvent être fulgurants, son intégration dans la manœuvre opérationnelle globale est un processus qui se caractérise par une planification longue et très spécifique. Ces effets peuvent être d'ordre matériel – neutralisation d'un système d'arme – ou immatériel – collecte de renseignement , temporaires, réversibles ou définitifs.

2) LA FINALITÉ DE LA LIO : CONTRIBUER DANS LE CYBERESPACE À LA SUPÉRIORITÉ MILITAIRE

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.

Elle permet d'atteindre trois types d'objectifs opérationnels dans la conduite d'opérations militaires :

1) évaluation de capacités militaires adverses : recueil ou extraction d'informations ;
2) réduction voire neutralisation de capacités adverses : perturbation temporaire ou création de dommages majeurs dans les capacités militaires adverses ;
3) modification des perceptions ou de la capacité d'analyse de l'adversaire : altération discrète de données ou systèmes, exploitation d'informations dérobées au sein d'un système d'information militaire de l'adversaire.

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[3] ou en imposant une diversion de ses efforts vers des cibles inutiles.

Complémentaire des armes conventionnelles, la LIO produit les mêmes effets de renseignement, de neutralisation ou de déception tout en opérant dans un nouveau domaine.

3 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.

Elle peut être employée en substitution ou en combinaison des autres capacités de recueil ou d'action sur tout le spectre de l'engagement militaire : renseigner, défendre, agir :

RÔLE DE LA LIO DANS LES FONCTIONS OPÉRATIONNELLES

<table>
<tr><th>RENSEIGNER</th><th>DÉFENDRE</th><th>AGIR</th></tr>
<tr><td>Caractériser et attribuer des systèmes adverses</td><td>Identification de l'attaquant</td><td>Contrer la désinformation</td></tr>
<tr><td rowspan="2">Surveiller l'adversaire</td><td>Riposte.Intervenir dans l' espace numérique en cas d' intrusion</td><td rowspan="2">Accompagnement de la manœuvre militaire par la perturbation ou la neutralisation des capacités militaires de l'adversaire</td></tr>
<tr><td>Neutralisation conformément à l' Art. L. 2321-2 du code de la défense</td></tr>
</table>

3) L'ORGANISATION DE LA LIO : UNE CHAÎNE DE COMMANDEMENT UNIFIÉE, DES UNITÉS SPÉCIALISÉES

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 de la manœuvre interarmées. Il assure la cohérence de la planification et de la conduite des actions de LIO avec les différents états-majors opérationnels (interarmées, terrestre, naval, aérienne, forces spéciales), et les services de renseignement, ceux du niveau stratégique jusqu'au niveau tactique. Enfin, il développe et anime le volet LIO de la coopération militaire avec les alliés.

L'emploi de la LIO se conçoit aux niveaux stratégique (dans la manœuvre opérationnelle interarmées globale) et tactique (dans la manœuvre des composantes d'armées sur les théâtres d'opération).

EXEMPLES D'EMPLOI DE LA LIO AU NIVEAU TACTIQUE ET AU NIVEAU STRATÉGIQUE

	Emplois de niveau tactique	Emplois de niveau stratégique
Evaluation des capacités adverses	- Renseignement d'intérêt immédiat lié à l'action des forces	- Renseignement en préparation des opérations, à fins de ciblage ou de développement capacitaire
Réduction voire neutralisation de capacités adverses	- Neutralisation d'un système d'arme - Neutralisation d'un poste de commandement	- Neutralisation d'une capacité opérationnelle adverse (exemple : vecteur de propagande), - Neutralisation d'un système de commandement de niveau stratégique
Action sur les perceptions ou la capacité d'analyse adverse	Altération des données d'un système de commandement	- Désorganisation des centres de propagande adverses

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. L'action de ces unités spécialisées est pleinement intégrée à la manœuvre des armées, directement sur le terrain ou à distance.

MAÎTRISER LES RISQUES LIÉS À L'EMPLOI DE LA LIO : une condition *sine qua non* de toute opération

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.

Les risques liés à l'emploi de la LIO proviennent en premier lieu des caractéristiques propres au cyberespace : immédiateté de l'action, dualité des cibles et hyper-connectivité.

En outre, les moyens et modes d'action sophistiqués conçus en vue de mener ces actions nécessitent une maîtrise et un contrôle stricts de leur utilisation de bout en bout, notamment afin d'éviter tout risque de détournement, de compromission ou de dommage collatéral. En effet, une action de LIO peut propager ses effets au-delà de la cible visée en raison des inconnues de configuration et des interdépendances entre systèmes, de plus en plus courantes dans le cyberespace. Par ailleurs, un outil de LIO peut être volé, copié ou imité par des adversaires ou des acteurs tiers. Il ne présente généralement pas les contraintes associées à des armes de seuil réservées aux États possédant une certaine maturité technologique.

Enfin, les adversaires disposant de capacités offensives, mais qui offriraient une surface de vulnérabilité numérique moins étendue pourraient s'engager à moindre risque dans une escalade conflictuelle contre nos intérêts.

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 affaire de décision 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.

ENCADRER JURIDIQUEMENT L'ACTION DE LIO : une nécessité et une protection

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.

Lorsqu'elles sont menées en appui de la lutte informatique défensive, les actions de LIO sont conduites, sous la responsabilité du chef d'état-major des armées, dans le cadre défini en droit interne par le code de la défense et dans les conditions fixées par le Premier ministre.

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.

DÉVELOPPER UNE CULTURE PARTAGÉE DE LA LIO : des effets à intégrer en coalition

La France est un acteur majeur des partenariats otaniens et européens dans le domaine cyber.

La coopération dans le cyberespace ne va pas de soi et s'inscrit dans une logique complexe. Face à la menace cyber, les disparités de capacités, d'organisation, de doctrines et d'investissements des partenaires constituent une difficulté supplémentaire. C'est pourquoi, en 2016, dans le cadre de l'OTAN, la France et ses alliés ont signé un engagement invitant les pays membres à se doter de moyens cyber en vue d'assurer leur sécurité individuelle et par suite collective : le *Cyber Defense Pledge*. Dans la continuité de cet engagement, la France s'est engagée, comme ses principaux partenaires, à partager les effets produits par ses moyens propres de LIO à des fins de défense ou d'opérations militaires collectives, mais en gardant toujours la maîtrise et le contrôle national car ils relèvent de notre stricte souveraineté.

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.

Les engagements internationaux de la France dans le domaine cyber, illustrés par la signature de MoU ou d'agréments techniques encadrant la coopération, témoignent de la volonté de construire une politique de cyberdéfense avec des partenaires internationaux sur l'ensemble du spectre (LID et LIO) ; condition aujourd'hui indispensable à la défense de nos intérêts stratégiques.

RELEVER UN DÉFI POUR L'AVENIR : la LIO, une capacité militaire d'emploi à développer

Le développement des capacités de lutte informatique offensive au profit des armées est confié à la direction générale de l'armement (DGA), comme pour toute autre capacité militaire. En raison de la sensibilité et de la dynamique du domaine, les équipes du COMCYBER 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.

La LIO doit poursuivre son développement autour de cinq défis principaux :

- **accélérer la production de moyens** de lutte informatique offensive au profit des armées ;
- **définir une politique RH** qui permettra de répondre aux enjeux d'expertise de cette nouvelle capacité ;
- **engager des actions de formation** à l'emploi de la LIO à des fins militaires, au sein des états-majors de planification et de conduite des opérations interarmées ;
- **adapter nos processus d'acquisition et de développement capacitaires** à la dynamique et la célérité de l'innovation du monde cyber ;
- **converger avec des partenaires, notamment européens, sur des ambitions opérationnelles** pour nous permettre d'agir en coalition y compris avec de la LIO sur un théâtre de crise.