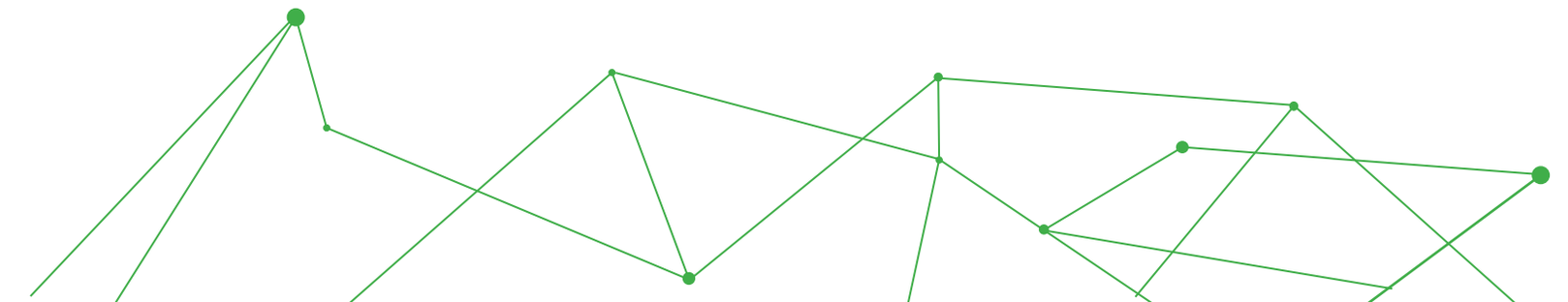
MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

ÉLÉMENTS PUBLICS DE DOCTRINE MILITAIRE DE LUTTE INFORMATIQUE D'INFLUENCE (L2I)

SOMMAIRE



PRÉAMBULE

Si dans le passé les conflits armés s'inscrivaient dans un continuum paix - crise - guerre, nous devons désormais envisager et préparer notre stratégie militaire selon le triptyque compétition - contestation - affrontement, plus pertinent pour aborder la conflictualité dans sa nouvelle complexité. En effet, la compétition entre grandes puissances s'est durcie et certaines puissances stratégiques ou régionales se sont enhardies et désinhibées. La guerre de l'information procède directement de cette nouvelle donne.

Profitant des opportunités offertes par le cyberespace, le nombre et l'intensité des attaques menées dans ce milieu ne cessent de croître, visant le profit financier, la paralysie de systèmes étatiques ou privés, la captation de données ou la déstabilisation des institutions par la manipulation des opinions. Poursuivant les objectifs de la Revue stratégique de défense et de sécurité nationale de 2017, réaffirmés dans l'Actualisation stratégique de 2021, le ministère des Armées construit les capacités permettant à nos forces d'évoluer dans un cyberespace de plus en plus contesté.

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.

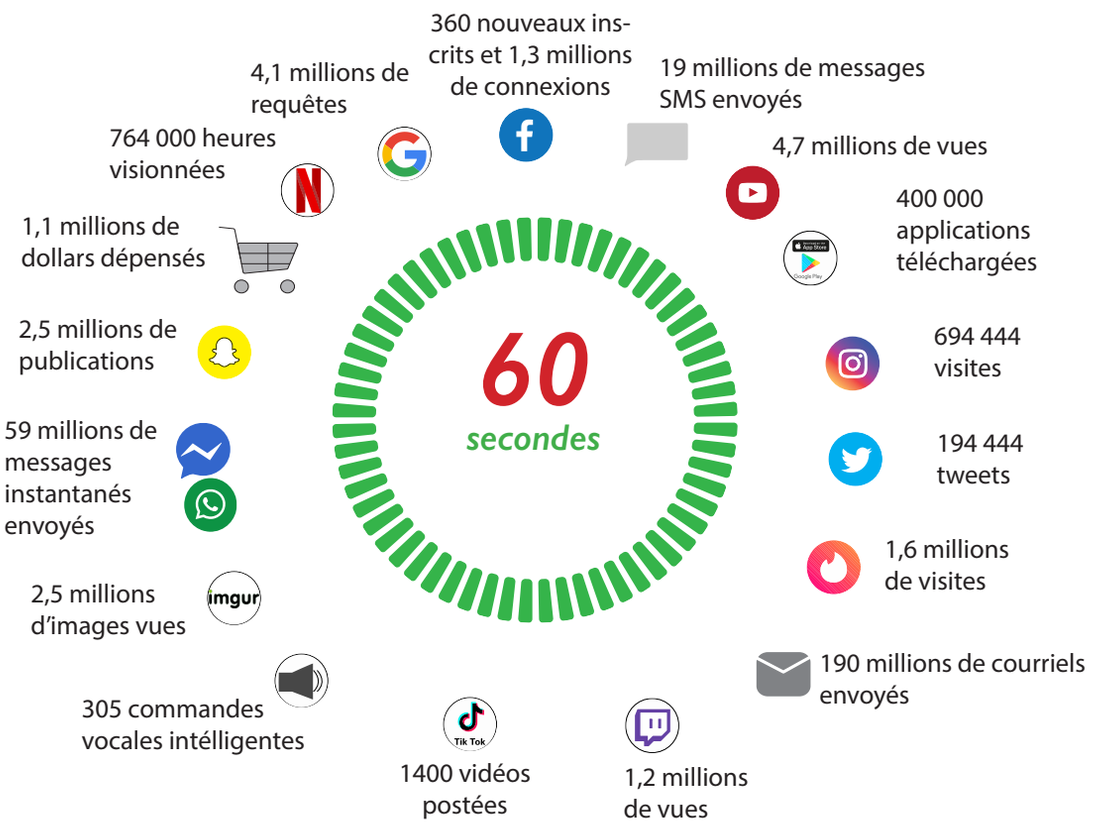
Engagées sous l'autorité du Président de la République sur les théâtres d'opération et dans des missions de souveraineté et de protection du territoire national, les armées françaises font l'objet d'attaques informationnelles dans le cyberespace, orchestrées par des groupes ou des États hostiles à leur action. Comme l'expose le chef d'état-major des armées dans sa vision stratégique[1], il s'agit de faire de nos armées des forces plus agiles, capables de faire face aux nouvelles menaces. En un mot : « gagner la guerre avant la guerre », tout en étant en mesure de la conduire s'il le fallait. Pour y contribuer, les armées disposent désormais d'une doctrine de lutte informatique d'influence (L2I) qui organise et structure ce type de 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.

Ce document complète le corpus doctrinal de cyberdéfense après la publication en 2018 de l'instruction ministérielle relative à la politique de lutte informatique défensive (LID), puis celle en 2019 d'une doctrine militaire de lutte informatique offensive (LIO).

[1] Vision stratégique du chef d'état-major des armées, octobre 2021

LE CYBERESPACE, NOUVEAU LIEU DE LA GUERRE DE L'INFORMATION

1) L'AVÈNEMENT DES MÉDIAS SOCIAUX A PROFONDÉMENT MODIFIÉ L'ENVIRONNEMENT DES OPÉRATIONS MILITAIRES



L'importance prise par les médias sociaux dans la vie quotidienne engendre un changement de paradigme majeur, qui touche aussi les opérations militaires : l'environnement informationnel numérisé est omniprésent dans les opérations, il marginalise les autres sources d'information et affaiblit la mise en perspective des informations.

Ce phénomène affecte jusqu'à nos processus décisionnels. Au-delà de nos vies professionnelles, nous en faisons un usage quasi permanent pour nos loisirs ou nos communications personnelles.

Propriétaires d'algorithmes de personnalisation qui permettent de trier, hiérarchiser et mettre en avant une information, les grandes entreprises du numérique jouent un rôle central dans ces transformations. De façon mécanique et pour des raisons souvent commerciales, ces algorithmes favorisent la création de communautés et orientent la façon dont chacun s'informe.

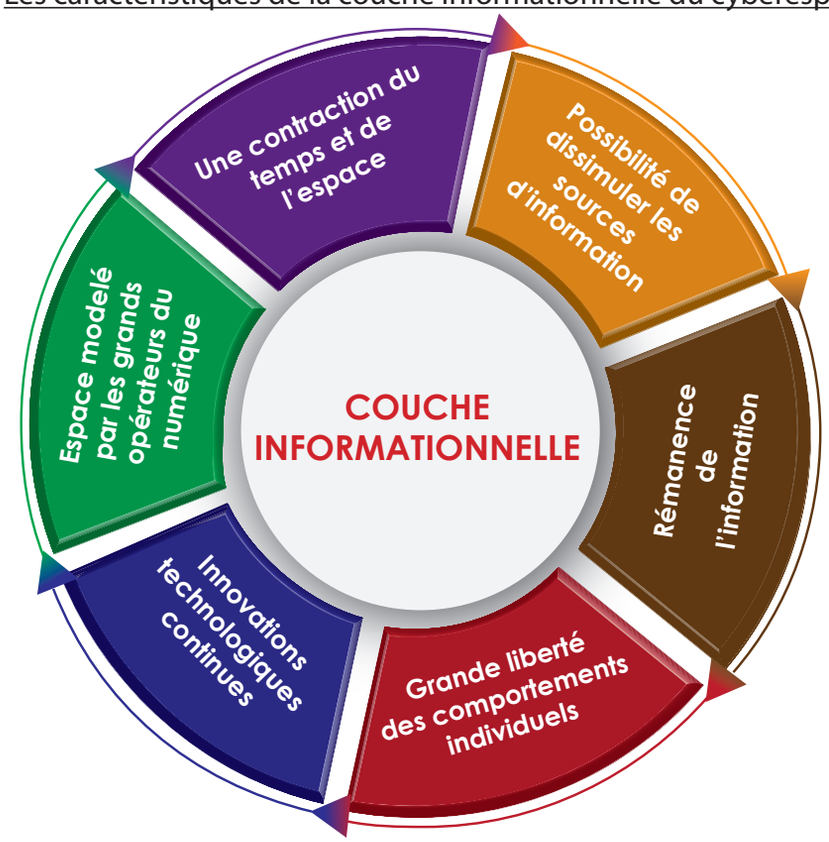
Ces évolutions sociétales influent sur le déroulement des opérations militaires.

Dans cet espace déterritorialisé, tout individu, groupe ou État peut, par sa seule capacité de conviction, acquérir une légitimité au sein d'un réseau qu'il peut ensuite aisément influencer. Cette influence participe de la stimulation émotionnelle des utilisateurs, ce

qui lui confère une dimension irrationnelle. Nos adversaires n'hésitent plus à utiliser cette arme contre nos opérations.

Si la guerre est avant tout caractérisée par des actions de combat, elle est aussi le choc de deux volontés concurrentes et antagonistes. À chaque étape d'un conflit, les protagonistes tentent de s'imposer mutuellement leur volonté, par des messages directs ou indirects, pour promouvoir leurs objectifs ou positions respectives et gagner des soutiens (population, alliés…) tout en cherchant à réduire ceux de l'adversaire. Le cyberespace est devenu le terrain de ces opérations de déception, et pour certains acteurs le terrain d'opérations de désinformations.

Les caractéristiques de la couche informationnelle du cyberespace



L'immédiateté de l'information, diffusée à très grande échelle, favorise l'interactivité. Les frontières géographiques de l'information et les délais de transmission s'effacent.

Dans le cyberespace une information est difficile à effacer car aisément dupliquée ou stockée ailleurs : elle peut donc être réutilisée hors de tout contexte vérifiable.

Innovation continue en matière de création, stockage et diffusion d'informations. Certaines des innovations en cours de développement ou d'appropriation (deepfakes[1], intelligence artificielle[2], réalité virtuelle ou réalité augmentée…) font émerger un nouvel espace numérique.

La maîtrise des technologies afférentes permet d'en dissimuler ou d'en falsifier les origines. Cette anonymisation croissante favorise l'utilisation du cyberespace par des États ou des groupes d'individus à des fins d'influence.

N'importe qui peut produire et diffuser de l'information, vraie ou fausse, sans aucun contrôle éditorial, ce qui favorise une production débridée d'information.

Opérateurs qui, de facto ; imposent leur propre réglementation. Le caractère dématérialisé du cyberespace complexifie l'application du droit.

[1] Deepfake ou hypertrucage : technique d'images de synthèse s'appuyant sur l'intelligence artificielle qui permet de modifier des images ou des vidéos en superposant et combinant de nouvelles images d'une façon qui semble authentique (par exemple, pour créer un faux discours d'un responsable politique ou de fausses exactions de soldats en opérations).
[2] Certains mécanismes pourront en effet être automatisés, notamment la production d'articles dans un champ sémantique, ou encore l'utilisation d'avatars automatisés capables d'interagir avec des comptes animés par des personnes réelles.

2) LA GUERRE DE L'INFORMATION, UNE RÉALITÉ DÉJÀ QUOTIDIENNE POUR LES ARMÉES

Un exemple d'attaque informationnelle sur Facebook contre l'opération Barkhane : circulation de fausses informations visant à faire croire que des militaires français pillent des ressources au Mali.

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. Depuis une dizaine d'année, des groupes terroristes et des États désinhibés y mènent des opérations. Ainsi, la France et ses armées constatent, en particulier depuis les attentats de 2015, des appels à la violence et au recrutement dans les mouvements terroristes ainsi que des actions de manipulation de l'information.

Les manipulations de l'information s'inscrivent typiquement dans le cadre de stratégies hybrides[1] 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. 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.

<u>Typologie des acteurs menaçant les forces armées :</u>

- des structures étatiques ayant pour finalité, lorsqu'elles ciblent des États, de les déstabiliser, de fragiliser leur cohésion ou encore de discréditer les pouvoirs publics. Nos armées sont aujourd'hui confrontées en opération à des attaques informationnelles ou des stratégies narratives étatiques sophistiquées, utilisant parfois des intermédiaires ;

- des groupes armés organisés, des groupes armés terroristes et des quasi-États qui exploitent le levier informationnel à des fins de propagande, de financement, de recrutement ou de coordination pour nuire à leurs adversaires.

[1] 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 risposte ou de conflit ouvert et dans le cadre d'une possible gestion d'escalade ».

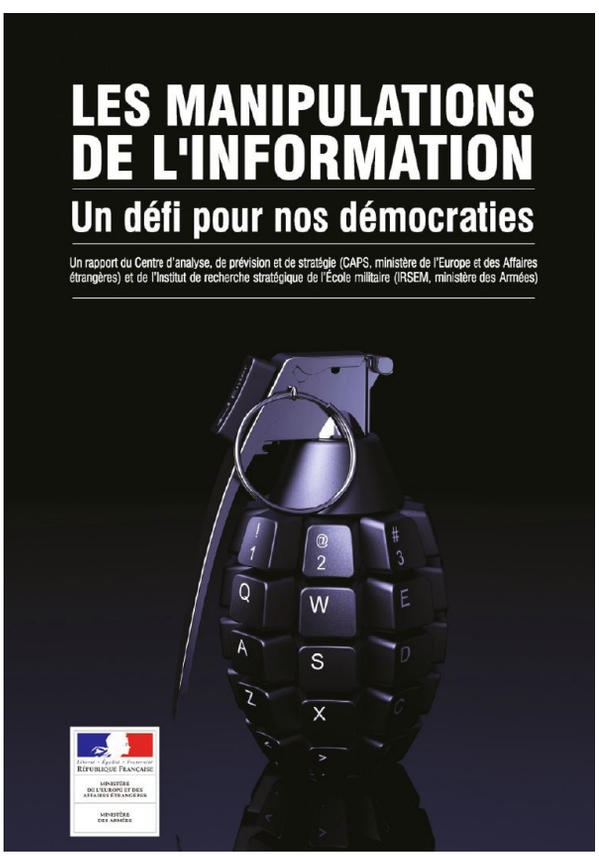
3) LA SUPÉRIORITÉ DANS L'ESPACE INFORMATIONNEL, ENJEU POUR NOS ARMÉES

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.



En 2018, le Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et l'Institut de recherche stratégique de l'École Militaire (IRSEM) ont publié ce rapport sur les manipulations de l'information.

LA LUTTE INFORMATIQUE D'INFLUENCE (L2I)

1) DÉFINITION

La lutte informatique d'influence (L2I) désigne les opérations militaires conduites dans la couche informationnelle du cyberespace pour détecter, caractériser et contrer les attaques, appuyer la StratCom, renseigner ou faire de la déception, de façon autonome ou en combinaison avec d'autres opérations.

Le lieu d'action de la L2I est la couche informationnelle[1] du cyberespace. Du fait des caractéristiques de cet espace, sa maîtrise requiert des compétences communes avec celles de la LID et de la LIO.

Les opérations de L2I contribuent à la communication stratégique (StratCom[2]) ministérielle. Ce sont des opérations militaires commandées par le chef d'état-major des armées qui, comme pour les opérations de LID et LIO, en délègue le contrôle à l'officier général commandant de la cyberdéfense (COMCYBER)[3]. Elles consistent, pour l'essentiel, à détecter les attaques informationnelles susceptibles de nuire à la réputation des armées ou d'entraver leur action, à les caractériser, à les contrer et à promouvoir l'action de nos forces. La L2I peut aussi offrir, sur nos théâtres d'opérations, des opportunités de recueil de renseignement et d'opérations de déception qui doivent être pleinement exploitées.

Conformément aux engagements pris par la France, ces opérations sont menées dans le strict respect du droit, national et international. Le développement des capacités afférentes, d'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.

---

[1] Le cyberespace se structure en trois couches indissociables d'où procèdent toutes les menaces :
- une couche physique, constituée des équipements, des systèmes informatiques et de leurs réseaux ayant une existence matérielle (donc une territorialité qui ouvre sur un droit national voire international) et, pour certains d'entre eux, une existence électromagnétique ;
- une couche logique, constituée de l'ensemble des données numériques, des logiciels, des processus et outils de traitement, de gestion et d'administration de ces données, ainsi que de leurs flux d'échanges, implantés dans les matériels pour leur permettre de rendre les services attendus ;
- une couche cognitive, également appelée couche « cognitive » ou « sémantique », constituée des informations et des interactions sociales de toutes sortes qui se trouvent dans le cyberespace et des personnes qui peuvent déclarer plusieurs identités numériques. Cette concentration d'informations fait de la couche cognitive une interface majeure avec les autres couches du cyberespace, les populations et leur environnement informationnel.

[2] La communication stratégique (ou StratCom) des armées est le processus qui permet de cadrer la conception et la conduite de toute activité militaire des armées françaises comme un message cohérent, crédible et efficace auprès des principaux acteurs qui en ont connaissance, qu'il s'agisse d'une action physique ou d'une prise de parole sous toutes ses formes (Doctrine interarmées DIA-3.10(A)_ du 23 juin 2014, amendée le 12 mars 2018).

[3] Ce contrôle peut être délégué ou adapté dans des circonstances particulières.

2) OBJECTIFS ET TYPES D'OPÉRATIONS MILITAIRES

	RENSEIGNER	DÉFENDRE	AGIR
Objectifs militaires	- Connaître l'environnement informationnel d'une opération militaire - Détecter et caractériser les attaques informationnelles adverses - Connaître les intentions et les dispositifs militaires adverses	- Contrer les attaques informationnelles adverses s'opposant à l'action de nos forces pour les faire cesser ou en atténuer les effets	- Valoriser l'action de nos forces armées dans leur zone d'action - Affaiblir la légitimité de nos adversaires - Appuyer les opérations menées dans le champ physique par des manœuvres de déception
Types d'opérations militaires	- Veille numérique - Induire l'adversaire en erreur pour lui faire dévoiler ses intentions ou son dispositif	- Dénoncer, contenir, affaiblir ou discréditer, y compris par la ruse, une attaque informationnelle	- Promouvoir l'action des forces armées sur les médias sociaux - Convaincre les acteurs d'une crise d'agir dans le sens souhaité - Dénoncer les incohérences ou mensonges de l'adversaire - Induire l'adversaire en erreur (opérations de déception)

UNE CHAÎNE DE COMMANDEMENT DEDIÉE

Sous l'autorité du Président de la République, le chef d'état-major des armées exerce le commandement des opérations militaires. Il est le conseiller militaire du Gouvernement.

Pour réaliser les opérations de L2I, il s'appuie sur le Commandant de la cyberdéfense (COMCYBER)[1] et sur des unités spécialisées.

1) RÔLE DE L'OFFICIER GÉNÉRAL COMMANDANT DE LA CYBERDÉFENSE (COMCYBER) DANS LES OPÉRATIONS DE L2I

La L2I s'exerçant dans le cyberespace, ses opérations peuvent se combiner avec celles de la LID et de la LIO[2]. Elles exigent un haut niveau de maîtrise des compétences spécifiques à ce milieu et une coordination centralisée au niveau stratégique.

Conduites dans le cadre d'un engagement des forces armées, les opérations de L2I sont partie intégrante de la manœuvre interarmées. S'inscrivant en cohérence avec la STRATCOM ministérielle, elles peuvent être coordonnées avec l'action d'autres ministères et, dans le cadre d'une opération interalliée, avec les structures dédiées développées au sein d'organisations internationales dont la France est membre ou constituées pour la circonstance.

La planification et la conduite des opérations de L2I dans cet environnement sont assurées par le COMCYBER, et intégrées dans les actions interarmées.

2) DES UNITÉS MILITAIRES SPÉCIALISÉES

La L2I se place à la confluence de la cyberdéfense et de l'influence.

Le Centre interarmées des actions sur l'environnement (CIAE) regroupe des acteurs français de l'influence militaire. Les ressources humaines et moyens techniques consacrés à la L2I sont concentrés en son sein, sous le contrôle opérationnel du COMCYBER.

Une comparaison internationale : aux États-Unis, le concept des WebOps

Chaque COCOM dispose d'un " WebOps ", une unité de veille et d'action numérique agissant en soutien d'une opération militaire par des actions dans la sphère informationnelle :

- soutien à la STRATCOM ;
- perturbation de la propagande adverse ;
- dénonciation des infox ;
- mobilisation des opposants de l'adversaire afin d'amplifier leurs actions.

[1] Créé en 2017, le COMCYBER assure la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées et la conduite de la défense des systèmes d'information du ministère. Sous l'autorité du sous-chef d'état-major « opérations » de l'EMA, il est responsable de la conception, de la planification et de la conduite des opérations militaires de cyberdéfense. Il est également en charge de coordonner la préparation de l'avenir et de contribuer à la politique RH du domaine cyber.

[2] Ainsi, une attaque informationnelle adverse peut comporter des tentatives de manipulation de l'information et des attaques par rançongiciels, nécessitant des réponses combinant L2I et LID.

LE RESPECT DU DROIT, GARANT DE L'EMPLOI MAÎTRISÉ DE LA L2I

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.

La construction et le fonctionnement du cyberespace impliquent un enchevêtrement des frontières et, par conséquent, une complexification de l'interprétation des dispositions juridiques.

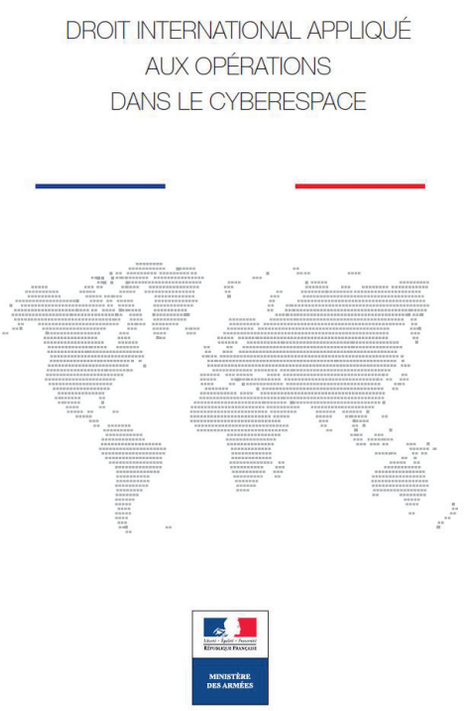
En 2019, la ministre des Armées a réuni un panel d'experts juridiques et l'a chargé d'établir un rapport sur l'application du droit international aux opérations dans le cyberespace. Ce rapport détaille la position française sur ce sujet. Il constitue une première, la France étant alors le seul pays à s'être formellement exprimé sur la question.

Les opérations militaires de L2I s'inscrivent dans ce cadre :

- en temps de paix, elles respectent la Charte des Nations unies et le principe de non-ingérence[1]. Elles s'inscrivent dans le cadre juridique applicable à l'engagement des forces armées.

- lors d'un conflit armé, elles respectent les règles du Droit international humanitaire (DIH), en particulier les principes fondamentaux de distinction, de nécessité militaire, de précaution et de proportionnalité dans l'attaque.

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.



Manuel sur l'application du droit international aux opérations dans le cyberespace, publié par le ministère des Armées en octobre 2019.

[1] Ainsi, il n'est pas envisageable par exemple d'influencer des processus électoraux étrangers.

DES DÉFIS POUR L'AVENIR : CONSOLIDER NOS CAPACITÉS DE L2I ET RENFORCER NOS PARTENARIATS

1) DÉVELOPPER LES RESSOURCES HUMAINES ET LES OUTILS DÉDIÉS

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. Il consacrera près d'1,7Md€ à ce nouveau domaine d'affrontement. Une partie de ces moyens sera consacré à la L2I.

Entre influence et cyberespace, la L2I requiert des compétences très variées et de haut niveau : spécialistes de l'environnement informationnel et cognitif, linguistes, infographistes, psychologues, sociologues, qui viennent s'ajouter aux combattants des armées.

La maîtrise du champ informationnel numérique requiert le maintien de connaissances au meilleur état de l'art dans les domaines techniques associés. La capacité à veiller des réseaux, à détecter des contenus et à analyser un environnement est liée à des outils spécifiques en constante évolution, utilisant les technologies de traitement des informations en masse (big data) et d'intelligence artificielle.

2) FAVORISER LES PARTENARIATS

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.

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Impression SGA/SPAC/Pôle Graphique de Paris