ASSOCIATION DE SOUTIEN À L'ARMÉE FRANÇAISE

"LA CYBERDÉFENSE"

MARS 2023

ASAF
ASSOCIATION DE SOUTIEN À L'ARMÉE FRANÇAISE

RÉDIGÉ PAR ADRIEN DE LA TOURNELLE
ÉTUDIANT EN MASTER 2, RELATIONS INTERNATIONALES

MAQUETTÉ PAR LAURE FANJEAU

LA SÉLECTION DES ARTICLES PROPOSÉS DANS CE DOSSIER A POUR SEUL OBJET D'OFFRIR UNE VARIÉTÉ D'ANALYSES QUI PERMETTRA AU LECTEUR DE SE FAIRE UNE OPINION PLUS STRUCTURÉE. ELLE N'ENGAGE AUCUNEMENT L'ASAF

CONTEXTE

La garantie de la souveraineté numérique de la France constitue un nouveau défi pour la Nation comme pour les armées. L'augmentation des attaques informatiques en témoigne. La plupart des luttes de pouvoir, des crises et des conflits contemporains connaissent aujourd'hui un développement dans l'espace numérique. Les armées intègrent désormais le combat cybernétique comme **un mode d'action à part entière** dont les effets se combinent aux autres dans une manœuvre globale, tout en continuant à distinguer le temps de paix du temps de conflit armé.

Enjeu et priorité stratégique, la **cyberdéfense est garante de la souveraineté nationale**. En lien avec de nombreux acteurs, le ministère des Armées participe activement à la protection, à la défense des systèmes d'information et à la conduite des opérations dans le cyberespace.

La compétition et la conflictualité ne se limitent plus, désormais, aux seuls milieux traditionnels, Terre, Mer, Air et Espace. Elles se sont étendues à ce nouveau champ au fur et à mesure que croissait l'utilisation des données numériques. **Le cyber est désormais envisagé comme arme d'emploi dans toutes les opérations.**

La revue stratégique de défense et de sécurité nationale de 2017 et la revue stratégique de cyberdéfense de février 2018 ont ainsi reconnu le **rôle majeur de la cyberdéfense militaire**. Cette consécration a trouvé sa traduction dans la Loi de programmation militaire 2019-2025 qui a acté l'augmentation significative des moyens financiers et humains à hauteur de 1,6 milliard et le recrutement de 1100 cybercombattants. Cet effort vient répondre à une nécessité qui se fait, chaque jour, plus pressante. Les travaux doctrinaux publiés en 2019 sur **la Lutte informatique défensive (LID) et la Lutte informatique offensive (LIO)** dans les opérations militaires complètent la stratégie de cyberdéfense et contribuent à la préparation de l'avenir des opérations militaires en intégrant graduellement cette nouvelle capacité à la manœuvre d'ensemble des armées.

Le terme de **cyberguerre** désigne généralement une cyberattaque ou une série de cyberattaques **menées par un pays contre un pays ennemi**. Toutefois, ces assauts peuvent aussi être menés par des organisations terroristes ou par des hackers soutenant un pays sans pour autant être enrôlés par son gouvernement.

Le but principal de telles offensives est de perturber, d'endommager, de dégrader ou de **détruire l'infrastructure informatique de l'ennemi**. Ces attaques peuvent potentiellement ravager l'infrastructure d'un pays, perturber des systèmes essentiels et causer de lourds dommages matériels voire même la perte de vies humaines.

La cyberguerre peut être utilisée à des fins d'**espionnage** ou de **sabotage**, par le biais d'attaques visant à endommager ou à détruire pour provoquer des pertes économiques ou des perturbations. **La propagande fait partie intégrante de cette guerre**, pour discréditer l'ennemi ou semer la discorde dans la population.

SITUATION

La cyberguerre n'en est qu'à ses balbutiements et il ne fait aucun doute que le pire reste à venir. Toutefois, plusieurs opérations ont déjà marqué l'histoire de cette nouvelle forme de guerre.

*** Stuxnet et le programme nucléaire iranien**

Apparu en 2010, **Stuxnet** est l'un des malwares les plus célèbres. Il aurait été **créé par les États-Unis et Israël**, même si aucun gouvernement ne l'a admis publiquement. Ce logiciel malveillant **cible les systèmes SCADA**, et aurait causé plusieurs milliards de dollars de dégâts au programme nucléaire de l'Iran.

*** Le piratage de Sony Pictures par la Corée du Nord**

Autre exemple : **le piratage de Sony Pictures par la Corée du Nord** en 2014, suite à la sortie du film « **The Interview** » qui ridiculise Kim Jong Un et met en scène son assassinat.

Un groupe dénommé « **Guardians of Peace** » a dérobé et dévoilé une montagne de données sensibles dont les numéros de sécurité sociale d'employés, des échanges d'email entre cadres... et des scripts de films à venir.

Même si la Corée du Nord nie sa responsabilité dans ce piratage, **le FBI a identifié des similitudes avec de précédentes attaques menées par ce pays dont le code**, les algorithmes de chiffrement et les mécanismes de suppression de données.

*** La statue du Soldat de Bronze en Estonie**

En avril 2007, des émeutes ont embrasé la capitale estonienne Tallinn suite à la décision de **relocaliser le monument soviétique du Soldat de Bronze hors du centre-ville**. Pour cause, de nombreux Estoniens percevaient cette statue comme un symbole de leurs souffrances pendant la Seconde Guerre mondiale.

Une série de cyberattaques s'en est suivie contre le gouvernement estonien et l'infrastructure essentielle du pays dont le parlement, les banques, les médias et les agences gouvernementales.

*** Les cyberattaques de la Russie contre l'Ukraine**

Depuis de nombreuses années, bien avant l'invasion militaire de 2022, la Russie multiplie les cyberattaques contre l'Ukraine.

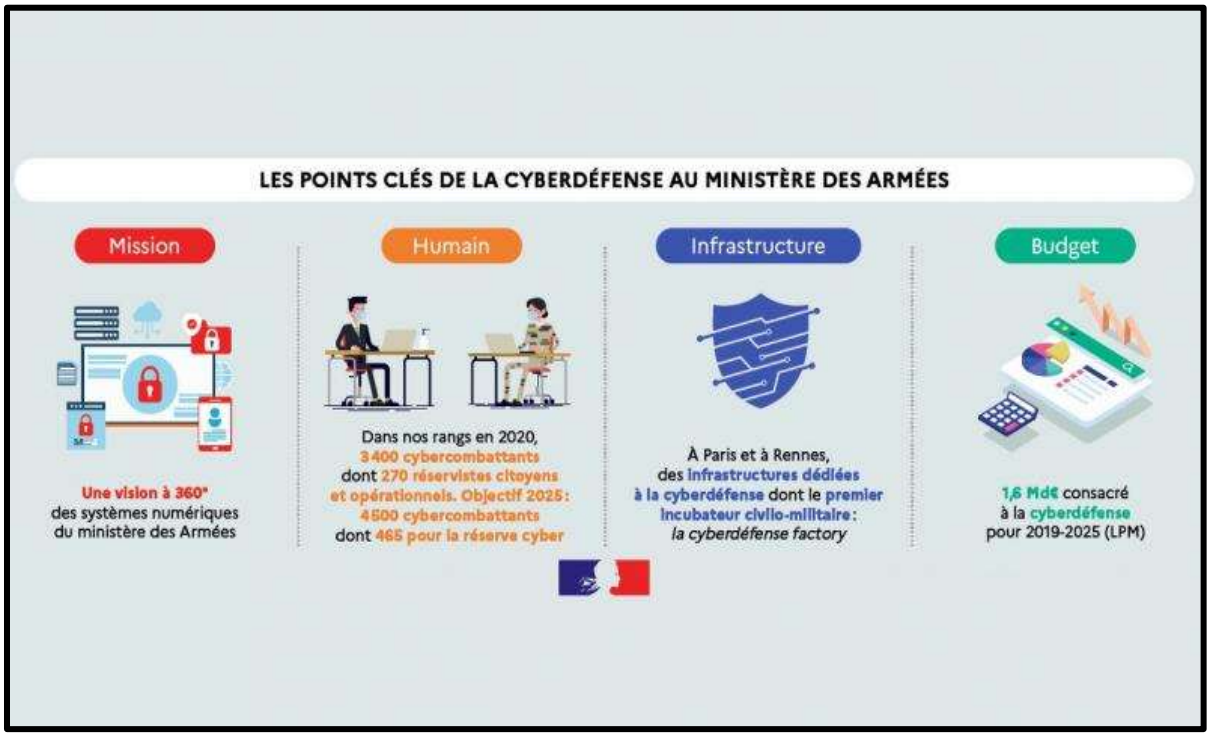
En juin 2016, **CrowdStrike** a accusé le groupe de hackers russe Fancy Bear d'avoir pris pour cible l'artillerie ukrainienne à l'aide du **spyware X-Agent** propagé via une application Android utilisée par l'armée. Cette opération aurait causé **la destruction de plus de 80% des Howtizers D-30** de l'Ukraine.

En décembre 2015, **les Ukrainiens** ont subi une série de pannes d'électricité durant plusieurs heures. Ce blackout fut causé par une cyberattaque contre le réseau électrique. La Russie a nié son implication, mais tout porte à croire qu'elle est à l'origine de cet assaut.

Depuis le début de la guerre en Ukraine, la Russie accompagne systématiquement ses assauts militaires de cyberattaques.

Source : cyberuniversity.com

DÉCLARATIONS OFFICIELLES ET ILLUSTRATIONS



Discours du président Emmanuel Macron, le 20 janvier à la base aérienne 118 de Mont-de-Marsan à l'occasion des vœux aux armées.

Ces formes de conflit prennent toutefois un nouveau visage qui oscille souvent entre la **sophistication et la simplicité brutale.** Sophistication avec une **course technologique, du cyber au quantique, en passant demain par l'intelligence artificielle.** Et brutalité presque nue, en Ukraine notamment, avec un retour de scènes que nous croyions appartenir à l'imagerie de Verdun ou de la Somme. Le **réarmement mondial** se fait donc aux **deux bouts d'un spectre polarisé**. **Entre la technologie de pointe et le rudimentaire,** qui peuvent malmener une armée puissante et bien équipée, mais vulnérable en haut et en bas de son champ d'action.
[…]
La guerre ne se déclare plus, elle se mène à bas bruit, insidieusement, elle est **hybride**. Le **ciblage d'infrastructures d'intérêt national mais civil** est notre lot commun, je pense entre autres aux **cyberattaques**.
[…]
La souveraineté, c'est aussi la **capacité de résistance**, notre résilience et d'abord la **résilience cyber**. Je souhaite que nous puissions **doubler notre capacité de traitement des attaques cyber** majeures.

Placé sous l'autorité directe du chef d'état-major des armées, le commandement de la **cyberdéfense** (COMCYBER) est un commandement opérationnel, **qui** rassemble l'ensemble des forces de **cyberdéfense** du ministère sous une autorité interarmées.

POINTS À SURVEILLER

Déclaration du PR le 20.01.2023, comment transformer les Armées ?

https://www.elysee.fr/emmanuel-macron/2023/01/20/transformer-nos-armees-le-president-de-la-republique-presente-le-nouveau-projet-de-loi-de-programmation-militaire

Les enjeux et l'importance du cyber

Quelle est l'importance du cyberespace ?

- CYBER : L'importance du cyberespace selon les généraux Bauer et Thierry Blanc https://www.asafrance.fr/item/cyber-l-importance-du-cyberespace-selon-les-generaux-bauer-et-thierry-blanc.html

Comment la menace stratégique s'est-elle concrétisée, accentuée et comment est-elle prise en compte au niveau international ? Quels progrès la France a-t-elle réalisés ? Comment placer la protection et la défense des systèmes d'information au cœur des priorités nationales et européennes ?

- Bockel, JM, 2012 ; Présentation du rapport La cyberdéfense : un enjeu mondial, une priorité nationale, sur Sénat.fr http://www.senat.fr/rap/r11-681/r11-68117.html

Le cyber est un enjeu fondamental. Quels ont été les progrès réalisés ? Quelles menaces planent sur la France ? Exemple du rançongiciel de l'hôpital d'instruction des armées Sainte-Anne, à Toulon. Comment renforcer notre chaîne de cyberdéfense ?

- Visualiser et télécharger le fichier Discours de Florence Parly - Montée en puissance du Commandement de la cyberdéfense - 7 septembre 2020

Les menaces

Quel est l'état de la menace cyber en France ?

- 2022, L'état de la menace cyber en France, site de la direction Générale de la sécurité intérieure. https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/cyberdefense/letat-de-la-menace-cyber-en-france

À quelles menaces la société fait face ?

- 2022, Principales menaces, site de l'ANSSI. https://www.ssi.gouv.fr/administration/principales-menaces/

La stratégie de défense et des responsabilités partagées

Comment définir la stratégie cyber des armées, selon Mme Parly, MINDEF ?

- Visualiser et télécharger le fichier Discours de Florence Parly - Stratégie cyber des Armées - 18 janvier 2019

Quels sont les dangers liés au monde cyber ? Quelle est la responsabilité de l'État dans la cyberdéfense de la Nation, et dans la garantie de la cybersécurité de la société ?

- 2018, revue stratégique de cyberdéfense sur sgdsn.gouv.fr http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

Quel est le rôle de l'UE dans la cyberdéfense ? Quelle place occupe la cyberdéfense dans les forces armées ?

- CYBER : Le général d'armée (2S) Marc WATIN-AUGOUARD revient sur l'accord européen MICNET https://www.asafrance.fr/item/cyber-le-general-d-armee-2s-marc-watin-augouard-revient-sur-l-accord-europeenne-micnet.html

Comment garantir la souveraineté du numérique ?

- 2022, Assurer la cybersécurité et coordonner la cyberdéfense, site de la SGDSN http://www.sgdsn.gouv.fr/missions/assurer-la-cybersecurite-et-coordonner-la-cyberdefense/

Qui protège les intérêts vitaux de la Nation contre les menaces cyber ?

- 2022, Le centre de cyberdéfense, site de l'ANSSI https://www.ssi.gouv.fr/agence/organisation/les-sous-directions/centre-operationnel-de-la-securite-des-systemes-dinformation-cossi/le-centre-de-cyberdefense/

En quoi la lutte informatique défensive est un défi collectif et nécessite une organisation optimisée, adaptée et comprenant une posture permanente ?

- Politique ministérielle de lutte informatique défensive, Comcyber et ministère des armées.
  Visualiser et télécharger le fichier Politique ministérielle de lutte informatique défensive

En quoi la lutte informatique offensive à des fins militaires offre une supériorité opérationnelle et constitue un défi pour l'avenir ?

- Visualiser et télécharger le fichier Lutte informatique offensive (LIO)

Quels outils pour lutter ?

Quelles sont les pratiques essentielles à connaître pour sécuriser ses outils (Ordinateur, téléphone…) ?

- Visualiser et télécharger le fichier Les 10 commandements Cyber

Quels sont les outils de l'Union européenne dans la lutte contre les menaces cyber ?

- CYBER : L'Europe renforce sa coopération dans la cyberdéfense https://www.asafrance.fr/item/cyber-l-europe-renforce-sa-cooperation-dans-la-cyberdefense.html

Comment tester la coopération des différents acteurs face aux menaces hybrides ?

- COOPERATION - Le COMCYBER participe à un exercice international de grande envergure de l'OTAN https://www.asafrance.fr/item/cooperation-le-comcyber-participe-un-exercice-international-de-grande-envergure-de-l-otan.html