Stratégie cyber de l'armée française : prendre le leadership européen

Introduction

Le 18 janvier 2019, la Ministre des Armées a prononcé un discours relatif à la stratégie cyber des armées françaises, accompagné de la publication d'un document sur la lutte informatique offensive. La mise en avant d'une doctrine publique, dans un domaine traditionnellement marqué par le secret, est pratiquement inédite.

Par un tel acte politique, la France cherche à accomplir plusieurs objectifs: affirmer sa place dans le contexte interallié, prendre le leadership européen, et faire entrer son appareil militaro-industriel de cyberdéfense dans une maturité nouvelle.

Afin d'accomplir ses objectifs, la France va devoir relever des défis d'ampleur: organisation administrative, construction de capacités techniques nouvelles, entraînement opérationnel. Si la France aligne des moyens substantiels, elle ne pourra faire l'économie d'une réflexion plus profonde sur son organisation interne et ses relations avec ses partenaires européens. Nous identifions des failles de l'organisation française et exprimons des propositions d'évolutions.

Une originalité française

Le caractère inédit de la démarche française ne doit pas être sous-estimé. A ce jour, aucune nation occidentale n'a assumé avec autant de clarté sa volonté de mener des actions de Lutte Informatique Offensive (LIO). Depuis ses origines, la cyberguerre a été la chasse gardée des services de renseignements extérieurs.

Ces institutions ont donc donné tout naturellement à cette activité un caractère clandestin. Cette **dimension clandestine** présente des intérêts majeurs pour le décideur politique: elle lui permet d'agir avec une grande rapidité, d'envoyer des messages politiques discrets à moindre coût; de plus, dans les démocraties occidentales, le contrôle parlementaire de ces activités reste souvent moindre. Si la France souhaite se défausser de cet atout, c'est qu'elle espère tirer des bénéfices politiques importants.

Sur le plan international, cette initiative doit être mise en perspective avec d'autres actes politiques majeurs. La France mène activement campagne, par le biais de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et du Ministère des Affaires étrangères (MAE), pour la mise en place de règles mondiales sur l'utilisation de l'arme cyber. Au cours du colloque *Cyber Defense Pledge*, Florence Parly a précisé qu'une agression cyber peut être constitutive d'un déclenchement de l'article 5 de la Charte de l'OTAN.

La doctrine française mentionne, comme motivations, de nombreuses attaques informatiques contre l'Estonie, l'Ukraine, l'Allemagne et d'autres nations occidentales. La France entend donc **prendre le leadership européen** par son intégration systématique dans les dispositifs défensifs, tout en revendiquant de **disposer seule d'un arsenal offensif** qui pourrait servir à accomplir des buts de portée européenne.

Cette doctrine publique permet de **mobiliser plus largement** au profit d'actions offensives. Il sera beaucoup plus simple pour la France de fédérer la diversité des énergies (laboratoires de recherches, industriels de l'armement, PME innovantes…) dans le cadre d'une capacité qui ne sera plus confinée au monde de la clandestinité.

L'entrée officielle de ce domaine dans le domaine militaire pourrait en faire un sujet sérieux de coopération d'armement, via des organisations telles que l'Organisation conjointe de coopération en matière d'armement (OCCAR) ou l'Agence européenne de défense (AED).

Cette doctrine publique a pour objet de **rassurer et légitimer**. L'exposé des emplois possibles mentionne des effets bien connus du monde militaire (renseigner, neutraliser, désorganiser). Par cette affirmation, la France démystifie le cyber, et cherche à l'inscrire dans le paysage connu et maîtrisé de la guerre moderne.

Elle est cohérente avec les efforts de la France pour faire entrer ce domaine dans le cadre du droit des conflits armés, ainsi que l'intégrer aux principes internationaux de sécurité collective.

Ce pari reste très risqué. Si la France peut imaginer rompre avec le consensus international, elle reste entourée de partenaires pour lesquels cette activité est avant tout liée au renseignement. Toute coopération opérationnelle ou technique se fera donc avec le **spectre de la coopération européenne de renseignement.** Quant à la possibilité de mobiliser plus largement, elle repose sur l'hypothèse que l'arme cyber peut prendre la forme de **projets lourds, aboutissant à des capacités maîtrisées**. Aucun exemple réel ne permet d'étayer cette hypothèse.

Une arme nouvelle et des défis nouveaux

La doctrine française reconnaît que l'arme cyber possède des caractéristiques propres (célérité technologique, prolifération simple des armes…).

Mais elle décide de traiter cette nouveauté avec beaucoup de classicisme. Ainsi, l'Etat-Major des Armées (EMA) portera l'emploi, et la Direction Générale de l'Armement (DGA) sera chargée de la production des armes. Certains défis associés sont identifiés:

- La nécessité d'adapter les processus d'acquisition et de développement capacitaire;
- La définition d'une politique RH cohérente;
- L'acculturation des opérationnels à cette arme;
- La convergence avec les partenaires internationaux.

Ces défis sont correctement identifiés. Les armées ont besoin de découvrir les capacités de cette arme, afin de l'intégrer dans leur processus de planification, et la DGA ne pourra se contenter d'assurer sa mission classique de maîtrise d'ouvrage dans un domaine si peu mature.

Néanmoins, ce modèle classique **se heurte à certaines réalités, que la doctrine française n'a pas véritablement intégré.**

Le recours à la séparation classique EMA -DGA pré-suppose que l'arme cybernétique est une arme au sens classique, dont on précise des caractéristiques et dont on fait l'acquisition. Or les attaques reposent sur des failles de fonctionnement, dont la durée de vie est souvent courte, et dont l'exploitation nécessite une connaissance fine de l'effet opérationnel.

Cela nécessite donc **l'intégration rapprochée de l'expert technique à l'opération.** Cette intégration est bien éloignée de la culture française en la matière.

Serait-il possible de disposer de cette expertise en interne? Rien n'est moins sûr, car la France se retrouve en concurrence avec des entreprises privées qui connaissent le prix du talent. Ainsi certaines vulnérabilités particulières peuvent s'échanger auprès de brokers pour plusieurs centaines de milliers d'euros. Et cela sans compter sur des grandes entreprises de la tech qui n'hésitent pas à offrir des salaires à 6 chiffres à des jeunes trentenaires.

Cette concurrence concerne d'ailleurs tous les métiers du cyber (analystes, développeurs, chercheurs…).

Au delà de la problématique salariale, les profils recherchés évoluent dans des communautés très internationalisées. Un expert se retrouvant coupé de son milieu, pour des raisons de confidentialité des missions, risquerait de perdre en compétence très rapidement. La France aura du mal à constituer une communauté technique autonome de niveau suffisant.

Au delà des profils d'experts techniques, la cyber nécessite des officiers en charge de mener les opérations associées, et de les intégrer plus globalement dans une manoeuvre militaire. Disposer de ces profils va nécessiter plus qu'une simple acculturation. Si le cyber est constitué d'équipements, de logiciels, de systèmes techniques, il est aussi un milieu. Le cyberespace déforme la géographie traditionnelle à laquelle sont habitués les militaires, et les confronte chaque jour à des choix pour lesquels ils ne peuvent être préparés par un autre milieu (terre, air, mer).

La France souhaite proposer un modèle intégré en coalition, qui reste très marqué par le contexte OTAN. La coopération opérationnelle européenne est quasi inexistante, et la France risque ainsi de se retrouver dans un **club anglo-saxon**, entourée de pays disposant de 10 ans d'avance sur la cyber. De plus, l'arme cyber brouille la ***distinction entre armement et emploi des armes***, obligeant les opérationnels à se confronter à des raisonnements propres à la diplomatie de l'armement.

Quelles évolutions ?

La France dispose d'atouts fondamentaux pour développer cette arme: des ingénieurs et des développeurs de qualité, des industriels de classe mondiale , une véritable compétence dans le domaine du renseignement technique, ainsi qu'une grande culture de l'indépendance.

Mais si l'arme informatique est bien une **arme à effet de levier,** elle représente donc bien une part minime dans le budget de la défense. La France peut être tentée, par facilité administrative, de plaquer sur ce domaine les schémas classiques de l'organisation de la défense.

Nous identifions cinq évolutions importantes nécessaires à la bonne prise en compte de ce domaine.

I – Faire évoluer les règles de participation des personnels civils et prestataires externes aux opérations militaires.

Les règlements existants ne permettent pas à des personnels civils, ou à des industriels de participer à des actes de combat, qu'il soit numérique ou non. Cette distinction ne pourra être à moyen terme dans le domaine cybernétique.

L'intégration expérimentale de tels personnels dans des structures opérationnelles pourrait passer par des "Security Operations Center" (SOC), ou par des opérations de Lutte informatique défensive (LID).

II – Créer une filière de formation spécifique pour des officiers cyber

Une telle filière, recrutant au milieu de scolarité des différentes écoles d'officiers, formerait des officiers d'ancrage "cyber" par un cursus spécifique et des stages dans des unités opérationnelles de cyberdéfense.

III – Lancer des programmes d'équipements cyber au niveau européen, en se reposant sur l'AED et l'OCCAR.

Des programmes européens d'équipements cyber permettraient de commencer à structurer une base industrielle et technologique de défense européenne, reposant sur une communauté technique et scientifique de niveau continental: une telle communauté pourrait disposer de la masse critique nécessaire, et pourrait fonctionner en confidentialité sur la base de mécanismes existants (Confidentiel UE, Confidentiel OCCAR).

De plus, les équipements ainsi produits seraient naturellement partageables entre les différents états membres, et pourrait constituer la base technique d'une capacité opérationnelle européenne.

IV – Faire évoluer les règles de recrutement et de rémunération des personnels de la défense impliqués dans le domaine.

Les règles de rémunération doivent permettre de valoriser les profils d'experts de très haut niveau, permettant d'être concurrentiel avec les entreprises privées. De plus, les carrières doivent permettre de valoriser l'expertise, et pas seulement les responsabilités managériales.

V – Expérimenter des modes d'acquisition nouveaux pour les équipements cyber à visée souveraine.

Certains besoins opérationnels ne pourront être remplis par l'organisation normale de l'acquisition d'armement. L'acquisition d'équipements cyber pourrait s'inspirer des mécanismes d'acquisitions utilisés par les unités de forces spéciales.

En conclusion, la France doit adapter son modèle à la guerre qu'elle entend mener demain, plutôt que d'essayer d'adapter la guerre à ce que son modèle actuel lui permet de mener.

Note rédigée par un contributeur du Millénaire.

Sources générales :

- *Elements publics de doctrine de lutte informatique offensive – Ministère des Armées*

Le Millénaire est un groupe de réflexion spécialisé sur les questions de politiques publiques et travaillant à la refondation de la droite. Il est composé d'une trentaine de contributeurs de divers horizons —cadres du privé, du public, chercheurs, chefs d'entreprises— et chacun expert dans son domaine.

Bureau du Millénaire :

Président : **William Thay**

Vice-Président : Gilles Bösiger

Secrétaire général : Florian-Gérard-Mercier

Secrétaire général adjoint : Pierre-Henri Picard

Secrétaire général adjoint : Olivier Bodo

Secrétaire général adjoint : Jean-Baptiste Gardes

Directeur de la Communication : Alexis Findykian

Contact :

William Thay : william.thay@lemillenaire.org
Florian Gérard-Mercier : florian.gerard-mercier@lemillenaire.org
Alexis Findykian : alexis.findykian@lemillenaire.org

Presse : presse@lemillenaire.org

Et pour suivre toutes les actualités du Millénaire :

http://lemillenaire.org

https://twitter.com/Le_Millenaire

https://www.facebook.com/Millenaire/