CEPS
Centre d'Étude et de Prospective Stratégique

26 février

Club Etat d'alerte Cyber

Les armées dans le substra numérique : Quelles missions ? Quels enjeux ? Quels axes stratégiques dans le temps de la loi de programmation militaire ?

❖

« *Porteur d innovation, le numérique est sans limite, il innerve tous les milieux physiques, il est devenu lui même un champ de confrontation à part entière, sa maitrise exacerbe les rivalité entre les puissances qui y voient un moyen d'assurer une supériorité sur le plan stratégique* » Cette déclaration du Président de la République, Emmanuel Macron, témoigne de l'importance accordée à la Cyber défense au plus haut sommet de l'Etat. Le **Commandement Cyberdéfense** en a fait une priorité. Un mot d'ordre : veiller aux enjeux d'une vision stratégique de souveraineté numérique.

L'ennemi ne porte pas de casque, ni d'uniforme, il est invisible et peut frapper insidieusement à tout moment. Son nom ? Le « Malware », logiciel malveillant, terme qui désigne une variété de logiciels hostiles ou intrusifs : virus informatique, vers, cheval de Troie, ransomware, spyware, adware, scareware, etc.

Face à cette menace permanente, le Ministère des Armées doit disposer de ce que l'on pourrait appeler des « munitions informatiques ».

Les « cyber attaques » peuvent impacter les systèmes et mettre en danger les intérêts supérieurs de la nation. Pour formaliser le risque d'atteinte à la souveraineté numérique de la France, un livre blanc a été rédigé qui part d'un constat : la « cyber menace » peut produire des effets globaux avec des ressources limitées.Cette nouvelle donne rebat les cartes des jeux de puissance sur l'échiquier international. Par le biais du cyber, des nations en perte de puissance sont en mesure de reprendre position sur l'échiquier international. Des pays peuvent, en effet, se hisser au niveau des plus grands en menant des actions pour imposer leur volonté.

Ce nouveau « champ de bataille » révèle également une certaine forme de **dépendance**. La numérisation des systèmes de commandement est une **chance** pour la conduite d'opérations. Elle crée un effet de surprise chez l'ennemi, elle accélère les actions pour peu que l'on ait bien préparé les frappes à l'avance. Le cyber permet des actions immédiates. Il facilite autant les frappes chirurgicales que les frappes de masse. Pourtant, cette numérisation génère aussi une certaine **vulnérabilité** en offrant un point d'entrée qui peut être utilisé par l'adversaire.

Au même titre que les entreprises ou les particuliers, l'armée est concernée par cette menace, à la différence notable qu'est en jeu la défense de la souveraineté nationale et la défense des intérêts supérieurs de la Nation. Au delà même d'une opération c'est toute son activité dans son ensemble qui peut être fragilisée par une « cyber attaque ». Fort de ce constat de fragilité, la Revue Stratégique de Cyberdéfense a pris a bras le corps cette question. Elle a structuré cette approche de la Cyberdefense en quatre chaines opérationnelles :

- **La chaine de protection.** En liaison avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) -service français créé par décret en juillet 2009- le Ministère des

Armées met tout en œuvre pour avoir des systèmes résilients tant sur le terrain national qu'à l'étranger, comme c'est le cas dans la lutte contre le terrorisme et Daech.

- L'action militaire. Sous l'autorité du Président Chef des Armées et le Commandant de la Cyberdéfense, la cyber est une arme offensive, un élément souvent décisif qui permet d'asseoir une supériorité opérationnelle sur les théâtres d'opérations. A cet égard, la France dispose d'une véritable doctrine qui permet de comprendre comment on peut utiliser des « capacités cyber » afin d'assurer la supériorité et la victoire des armes françaises dans les missions. Cette doctrine obéit à des règles strictes dans un cadre juridique avec des règles précises d'engagement et la prise en compte de mécanismes qui s'appuient sur le droit international et humanitaire. C'est notamment le cas lorsqu'il s'agit de pénétrer les systèmes de propagande de Daech et les casser en modifiant des éléments sans tomber sous le coup de la Loi.

- **La chaine de renseignement.** Il d'agit de protéger des informations vite accessibles et d'autres plus difficilement atteignables, mais qui présentent un risque de récupération.

- **La chaine d'investigation** (policière et judiciaire). Elle consiste en un arsenal d'actions appropriées pour qualifier les attaques et engager des actions.

La revue a également formalisé des **missions précises** et bien identifiées comme la prévention, l'anticipation pour se préparer aux attaques brutales, la protection (mécanismes de « fire walls »), la détection, l'attribution (décision politique) et la réaction (reconstituer les systèmes).

La mission du commandement de la cyber Défense

Depuis février 2017, le concept de **Cyber défense** a évolué à la mesure de la sophistication des attaques. Nous ne sommes plus seulement dans une approche technique, la démarche va bien plus loin avec des questionnements poussés sur les intentions de l' « attaquant ». De véritables plans de lutte défensive sont mis en place avec des profils « officiers cyber »

autour d'une nouvelle activité. Aujourd'hui, il n'est pas une opération militaire sans volet « cyber ». Au même titre que l'Air, la Mer, la Terre, les Forces spéciales, il y a désormais un Cyber système reconnu comme un corps à part entière.
L'activité Cyberdéfense veille à la protection des systèmes du Chef d'Etat major des armées et des systèmes de défenses dans une vision globale avec un cadencement de la manière dont l'on réagit. Les attaquants opèrent en entrant par des portes différentes et sont capables de fusionner des « bouts de cordes » pour attaquer le cœur du système.

Sur un plan opérationnel, il y a le siège du Commandement et des unités spécialisées regroupées à Rennes (Missions défensives, audit, et préparations opérationnelles) auxquels s'ajoutent des chaines de lutte informatiques défensives dans les organismes de la Défense. Ces enjeux sont opérationnels, mais aussi « capacitaires » et juridiques avec une doctrine qui définit les grands principes d'une politique de lutte informatique défensive et offensive pour le Ministère.
A la hauteur de ces objectifs, les ressources humaines et financières allouées s'inscrivent dans le cadre de la loi de programmation militaire. 1,6 milliard pour couvrir les besoins en investissements, fonctionnement et formation.

Plus de 1000 cyber combattants vont être formés jusqu'en 2025. Parmi eux, des professionnels de haut niveau qui, tels des « vigies », travaillent H24 pour observer l'activité des réseaux. Leur profil, plutôt bac +5 n'est pas seulement scientifique ou informaticien, mais géopolitique psychologie et littéraire pour pouvoir décrypter au mieux la diversité des « *attaques informationnelles* » (fake news) sur les réseaux sociaux. Dans la plupart des cas, c'est la légitimité des forces déployées qui peut être l'objet de mises en cause.

L'innovation est au cœur de la Cyberdéfense. Au delà de ce que fait traditionnellement, la DGA mise sur la notion d' « agilité ». Aller chercher des compétences est une priorité. En témoigne l'installation de la « Cyberdéfense Factory » à Rennes avec la mise à disposition de

données à des PME et start up pour qu'elles améliorent la performance des outils et se positionnent dans la recherche de solutions pour répondre à des besoins. Liens avec le secteur privé, « *fertilisation croisée* » avec les industriels, échanges avec des partenaires de confiance : l'un des enjeux de la Défense est son ouverture. Elle contribue à mieux faire monter son niveau de cyber sécurité collective.

Dans cette « guerre de l'information », quelques pistes de réflexion…

- **L'enjeu de la sémantique**

Pour pouvoir contre attaquer, encore faut-il pouvoir attribuer et caractériser. D'où l'importance de la dimension sémantique. Les livres blancs en 2012 et 2013 (30 000 pages !) ont défini un cadre juridique pour faire cesser des attaques. En 2015, Jean-Yves Le Drian, alors Ministre de la Défense, a contribué par ses prises de position a faire sortir ce concept de « l'ornière ». La **LIO** n'est plus un « tabou ». Le concept est accepté par opinion publique. La **lutte informatique offensive** (LIO) à des fins militaires, arme de supériorité opérationnelle, est l'ensemble des actions entreprises dans le cyberespace produisant des effets à l'encontre d'un système adverse, pour en altérer la disponibilité ou la confidentialité des données.

Compte tenu des menaces et des activités sur les réseaux sociaux –l'exemple du Mali et une activité numérique- pilotée par certains pays, il a fallu changer de conception stratégique. Affirmer l'excellence de la Cyberdéfense française et démontrer que les capacités offensives de la France peuvent dissuader un pays belligérant. Ce que l'on pourrait appeler la « dissuasion » ou le « découragement » de l'attaquant est une réalité.

- **La coopération internationale : à double tranchant**

Elle se révèle complexe. L'échange d'informations ne fait-elle pas courir le risque d'une perte d'informations pour un pays comme la France, bien placée dans la cyber sécurité ? Les « cybermenaces » ignorent les frontières. Les Etats, regroupés au sein d'organisations (Otan, Europe) sont conscients de la nécessité d échanger sans remettre en cause leur principe de souveraineté numérique. Les pratiques « one to one » sont devenues courantes entre militaires sur les "malware » et surtout les éléments de contexte. A une échelle plus large, la coalition militaire qui intervient sur le Levant est un exemple.

- **Où vont les données ?**

Dans la mesure où le moteur du numérique est la donnée, c'est toute l'architecture derrière les actions qui doit être pensée.Les éditeurs de logiciels sont des acteurs majeurs comme les grands operateurs des télécom. C'est dire l'importance de la confiance donnée à un partenaire à qui des données sont transmises. Doit on le faire avec un partenaire européen ou américain ? Ce n'est pas de la Cyberdéfense à proprement parler, mais cela conditionne aussi la sécurité numérique.

- **Quels coûts ?**

Les sommes engagées sont incontournables eu égard aux enjeux considérables. Dans ce domaine, il n'y pas de demi mesures face a l'ennemi. On peut neutraliser le décollage d'avions, le pilotage d'opération ou l'électricité. Ces actions peuvent assurer une suprématie opérationnelle. Par rapport au prix d'un système d'armes, les coûts sont minimes. Le ratio cout/attaque est de 1 à 50. Le plus cher, finalement, c'est l'humain. Il s'agit de recruter et faire monter en gamme la compétence générale face à la « cyberattaque ». Plus il y a de garde fous, moins l'attaque est rendue possible.