# La Cyberdéfense dans l'armée de Terre

***Général d'armée Thierry BURKHARD***
*Chef d'état-major de l'armée de terre*

Il y a moins de 30 ans, nos armées faisaient essentiellement la guerre sur terre, en mer ou dans les airs. Aujourd'hui, nous faisons de plus en plus la guerre dans les champs immatériels : champs informationnels, champs électromagnétiques, cyberespace. Posséder la supériorité dans ces champs interconnectés peut signifier posséder la supériorité tout court. En paralysant des systèmes d'armes ou en contrôlant des opinions, il est possible de faire plier un adversaire, en tout cas de le mettre en position d'infériorité.

Au cours de l'été 2019, dans le cadre d'un concours sponsorisé par le Pentagone, un groupe de hackers a créé l'événement en parvenant à « prendre le contrôle » d'un avion de chasse F-15 en moins de 48 heures. En introduisant un logiciel malveillant dans le système de commande de l'appareil, ces « pirates autorisés » ont réussi à empêcher le vol normal de l'avion, à capter les informations que recevait le pilote et à modifier la perception qu'il avait de son environnement.

Dans une autre mesure, les comptes Facebook, Twitter et TikTok de l'armée de Terre ont subi récemment plusieurs attaques dont deux sont assez emblématiques. Des groupes djihadistes sont parvenus à saturer nos réseaux sociaux de commentaires appelant à l'attaque d'Occidentaux. Plusieurs centaines de messages par minute ont été publiés durant plusieurs heures. Une autre attaque est aussi attribuable à des groupes birmans anti junte. Des milliers de commentaires ont été postés sur le compte TikTok de l'armée de Terre pour relayer leurs messages de lutte contre la répression.

Comment l'armée de Terre doit-elle se préparer à cette guerre dans les champs immatériels ?

La réponse peut paraître simple mais il s'agit de la même démarche intellectuelle que celle que nos armées ont dû conduire à travers toute leur histoire lorsqu'elles ont été confrontées à de nouvelles menaces et à de nouvelles armes.

**Nous devons définir aussi précisément que possible nos propres vulnérabilités tout en sachant saisir les opportunités offertes par les nouvelles technologies.**

Notre environnement voit tout d'abord l'affirmation d'une nouvelle forme de conflictualité. Les tendances de fond, identifiées depuis plusieurs années, ne font que s'accentuer. Nous observons le retour des rapports de force comme mode de règlement des conflits. La guerre entre l'Azerbaïdjan et l'Arménie aura fait 10 500 morts en 44 jours en octobre 2020 mais la crise sanitaire que nous traversons aura écarté notre attention de ce conflit et de ces chiffres terribles.

L'élévation du niveau technologique de nos compétiteurs est également un égalisateur de

puissance. L'Iran est aujourd'hui capable de réaliser des frappes de précision à longue distance comme il l'a montré avec l'attaque de la base américaine d'Al-Assad et à Erbil en janvier 2020 en Irak. Il est aussi capable de réaliser des attaques cyber relativement complexes, comme il semble l'avoir fait contre Israël au printemps dernier.

Enfin, dans un monde de compétition permanente, nous observons un emploi plus insidieux de la force, juste sous le seuil du conflit armé : action cyber, désinformation, harcèlement, etc. Les champs immatériels deviennent un espace de friction systématique, ce qui constitue, à mon sens, la rupture la plus importante dans la conflictualité moderne.

**Quelles menaces les champs immatériels représentent-ils pour l'armée de Terre ?**

Il existe tout d'abord **une menace technologique sur nos systèmes d'armes**. Entrées dans l'ère du « combat collaboratif », nos unités sont de plus en plus interconnectées. Elles échangent des informations d'un véhicule à l'autre : positions, comptes rendus d'observation, etc. Toutefois, à la différence d'un avion ou d'un navire, une force terrestre est très décentralisée et constitue un système « ouvert », qui est plus vulnérable du fait de ses multiples points d'entrée. De façon générale, la numérisation de nos systèmes d'armes accroît notre efficacité mais aussi notre exposition à la menace cyber.

Il existe ensuite **une menace sur la sécurité de nos informations**. Aujourd'hui, chaque véhicule détient en propre un nombre considérable d'informations. En pénétrant les systèmes d'information de nos unités, de nos états-majors ou de nos industriels, un adversaire peut apprendre énormément sur nos intentions ou de nos capacités.

Il y a aussi **une menace sur la crédibilité de nos opérations**. Au Sahel, nous faisons aujourd'hui face à des campagnes de désinformation orchestrées qui pourraient gravement compromettre la confiance que nous accordent la population et les gouvernements de la région.

Enfin, n'oublions pas que l'armée de Terre est en premier lieu un système d'hommes**. La dernière menace est donc sur l'humain.** Il y a 30 ans, en opération, nos soldats pouvaient passer plusieurs semaines sans donner de nouvelles et sans en recevoir. Dans nos casernes, on faisait la queue devant les cabines téléphoniques…

Aujourd'hui, quasiment tous nos soldats sont connectés grâce à leur montre ou leur smartphone. Cette hyper connexion peut conduire à un ciblage de nos soldats et ouvre la porte de la guerre informationnelle.

En 2018, la position de bases secrètes américaines était révélée sur internet grâce à l'application mobile de sport Strava, un réseau social de sportifs. Identifier un lieu de vie dans une base militaire et conduire une frappe cinétique ou informationnelle se trouvent désormais à la portée de tout ennemi même sans moyens et observation spatiale.

Avec la crise COVID, nous avons échappé à des campagnes de désinformation sur les réseaux sociaux à destination de nos soldats et des familles. Mais cela arrivera. Nos chefs, nos soldats et leurs familles doivent y être préparés.

**Dans ce contexte, l'ambition de l'armée de Terre et les défis qu'elle doit relever sont assez clairs.**

L'objectif est de ne pas subir les champs informationnels mais de nous y engager résolument et à tous les niveaux. Ne nous arrêtons pas seulement aux vulnérabilités, mais identifions aussi les opportunités que nous devons saisir. Nous devons durcir notre résistance à l'action de nos adversaires dans les champs immatériels. Nous devons avoir la volonté de ne pas leur laisser la libre possession des champs immatériels.

Nous devons être déterminés à y combattre à notre tour.

Nous avons donc **trois grands défis à relever** dont le premier est la bonne compréhension des enjeux.

**Il y d'abord un impératif d'acculturation de nos états-majors et de nos soldats.**

Historiquement et culturellement, nous sommes plutôt tournés vers l'action directe, cinétique. Nous devons évoluer dans notre approche opérationnelle et penser plus systématiquement aux champs immatériels, depuis le niveau de la section jusqu'à celui du corps d'armée. Quand nous penserons « manœuvre dans les perceptions », nous serons mieux préparés pour contrer les manœuvres adverses dans ce domaine.

Il ne faut surtout pas réduire les champs immatériels, et notamment le cyberespace, à une affaire de techniciens. Le cyberespace doit être envisagé comme l'espace terrestre. Nous manœuvrons dans le cyberespace, comme nous manœuvrons sur un champ de bataille : il faut se renseigner, se défendre, attaquer, etc.

Nous devons également recruter et former notre ressource sur un segment qui est devenu très concurrentiel. Nos entreprises sont effectivement très intéressées par les compétences de nos spécialistes qu'il nous faut toutefois fidéliser plusieurs années pour rentabiliser leur formation et surtout parce que nous en avons besoin.

**Le deuxième défi à relever est celui de la résilience de nos systèmes et de nos organisations.**

Continuer à structurer notre chaîne de cybersécurité pour protéger nos forces et notre industrie est un effort à poursuivre. En opération, nous déployons des détachements chargés de la protection numérique de nos unités. En métropole, nous montons aussi en puissance un centre de supervision des systèmes d'information métier de l'armée de Terre.

Mais il faut surtout penser notre sécurité des systèmes d'information (SSI) autrement. Nous ne pouvons plus construire des systèmes comme si rien ne pouvait y pénétrer. Un adversaire déterminé entrera toujours. Développer des systèmes résilients, capables de se reconfigurer est devenu un impératif. Penser la SSI comme une ligne Maginot est une vision dépassée et dangereuse.

Mais une fois de plus, n'oublions pas les hommes. Pour entraîner nos unités, il nous faut reproduire dans nos camps un environnement « cyber contesté » pour entraîner nos soldats.

Inversement, nous devons aussi nous entraîner à faire face « quand tout plante » : c'est ce que l'on appelle le mode dégradé. Même si nous utilisons des cartes numériques dans nos postes de commandement, nous continuons à mettre à jour nos cartes papier et nos cours de topographie commencent par l'apprentissage de la boussole avant celui du GPS.

Nos hommes doivent aussi être sensibilisés par leurs chefs aux informations qu'ils trouveront sur Internet. Un soldat bien entraîné, demain, sera celui qui sera capable de rendre compte s'il détecte ce qui lui semble être une campagne de désinformation sur Internet.

**Le troisième défi consiste à savoir et à pouvoir manœuvrer dans les champs informationnels.**

Il faut bien sûr être capables de conduire des attaques cyber au niveau stratégique, depuis la métropole. Nous devons aussi être en mesure de conduire ce type d'attaques depuis nos théâtres d'opération : c'est le niveau tactique. Nous devons déployer des capacités et les utiliser. Ce même effort doit être réalisé pour le brouillage. Ces capacités existent mais doivent être renforcées.

Notre capacité de guerre informationnelle doit, elle-aussi, être développée. Pour dissuader et décourager nos compétiteurs, nous devons être crédibles en affichant nos capacités militaires. Il nous faut savoir

détecter, caractériser et contrer les attaques informationnelles dont nous sommes la cible.

Nous devons intensifier notre communication stratégique sur notre posture, par exemple autour de nos grands exercices militaires et notamment avec ceux réalisés avec nos alliés. C'est ce que nous faisons avec l'opération LYNX dans les pays baltes. Le chargement de nos chars Leclerc dans nos bateaux de transport fait l'objet d'une manœuvre informationnelle planifiée en amont. Cela nécessite une grande anticipation pour avoir une parfaite cohérence de discours avec nos alliés.

Si nous n'acceptons pas de combattre dans les champs informationnels, d'autre le feront… contre nous. Nous nous y préparons et cela fait partie des axes d'effort de la vision stratégique que j'ai lancée il y a un an.