# Souveraineté numérique : le rôle des armées

Par le Vice-Amiral Arnaud COUSTILLIÈRE
Directeur général des systèmes d'information et de communication
du ministère des Armées

« *Les armées doivent planifier et conduire les opérations dans l'espace numérique jusqu'au niveau tactique, de façon totalement intégrée, à la chaîne de planification et de conduite des opérations cinétiques.*»

*Revue stratégique*, §299, octobre 2017

## Une souveraineté d'action

Le cyberespace est un milieu artificiel. Il se matérialise par trois couches : une couche physique (serveur, réseaux, terminaux), une couche logique (logiciel, automates, systèmes d'exploitation ou OS) et une couche cognitive (les informations, les liens sociaux). Un objet dans le cyberespace se retrouve dans ces trois dimensions. La dépendance des objets vis-à-vis de ces trois niveaux ne s'oppose pas à la fluidité des échanges. Bien au contraire, les facteurs qui compartimentent les autres espaces comme le temps et la distance sont ici gommés, voire inopérants, l'individu ou l'entreprise pouvant être touchés même au cœur du territoire national. Le milieu devient presque homogène. De cette homogénéité découlent une propriété d'ubiquité, un relatif anonymat et une rémanence. Ainsi, une donnée déposée sur le réseau pouvant se trouver simultanément en plusieurs endroits, il est très coûteux d'en retracer le parcours et illusoire de vouloir en effacer toutes les traces.

Appliquer une notion de souveraineté à un tel milieu n'est pas évident. Une approche consisterait à le comparer aux autres milieux mieux connus et maîtrisés. La souveraineté entendue comme terrestre ou terrienne est une souveraineté d'appartenance. La maîtrise du milieu s'y fait par une occupation permanente du sol. Lorsque l'homme a « conquis » les mers, il a défini une nouvelle notion de souveraineté : une partie de cet espace relève d'une logique de continuité territoriale, mais la haute mer n'appartient à personne, les bâtiments relèvent de leur pavillon. Pour y tenir sa place, l'État y envoie des navires et en assure la surveillance par intermittence : il s'agit d'une souveraineté de présence. Le milieu aérien est quant à lui une prolongation du milieu survolé ; il répond à une souveraineté d'appartenance ou de présence selon les endroits. Mais le cas des aéroports est intéressant lorsqu'on réfléchit à la notion de souveraineté : il illustre un « passage » dont le contrôle doit rester fluide. La souveraineté y est un mélange d'appartenance et de présence complété par une logique d'accès. Enfin, l'espace a sa logique propre puisque la souveraineté spatiale est purement une souveraineté d'accès. L'État est souverain spatialement quand il peut accéder librement à l'espace.

Le cyberespace, quant à lui, n'est à personne mais tout le monde y a accès. Il est matériellement implanté sur un territoire. Aussi, certains États font le choix d'une territorialisation d'Internet afin de mieux contrôler leur cyberespace. C'est le choix de la Russie, de l'Iran ou de la Chine, mais pas celui de la France et des nations occidentales. En comprenant le cyberespace comme un espace de liberté mais aussi de droit, l'État français définit l'ambition de sa souveraineté pour les armées comme la capacité de conduire en propre tout processus numérique d'intérêt national dans le cyberespace, sans y appliquer un contrôle permanent. Cette forme de souveraineté peut être qualifiée de souveraineté d'action.

## L'ambition numérique du ministère

L'exercice de la souveraineté se traduit par une stratégie qui s'intègre efficacement dans le déploiement de la politique numérique de l'État. Le rôle des armées dans la cyberdéfense a été présenté dès le Livre blanc de 2008 [1], puis confirmé avec de nouvelles ambitions dans celui de 2013 [2]. Depuis lors, le Premier ministre Manuel Valls a défini les objectifs de la stratégie nationale pour la sécurité du numérique en 2015 [3], le ministre de la Défense Jean-Yves Le Drian a créé un commandement Cyber (COMCYBER) en décembre 2016 [4], soulignant que « l'arme cyber est une arme à part entière, qui fait partie des moyens à disposition du commandement militaire ». Le fait « cyber » a aujourd'hui toute sa place dans la politique de défense de la France. À ce titre, la dimension numérique est présente tout au long de la *Revue stratégique de défense et de sécurité nationale* présentée en octobre 2017 [5] au président de la République.

Par ailleurs, sur un plan plus large, intégrant les opérations mais également le quotidien des personnels et l'amélioration de la relation au citoyen, la ministre des Armées, Florence Parly, a validé en novembre 2017 le document *Ambition numérique* [6] : « La révolution numérique sera un vecteur fort de cette transformation. Je veux la mettre au service du ministère : l'Internet des objets, l'intelligence artificielle ou le *Big Data* sont autant de chantiers ouverts sur lesquels nous devons appuyer le succès de nos armes, l'efficacité et l'excellence dans la conduite de toutes les missions du ministère. »

La révolution numérique en cours est un puissant moteur de transformation et d'accélération de la performance pour toute grande organisation. Le ministère et les armées ont résolument pris le tournant et saisi cette opportunité pour rester à la pointe des meilleures technologies et pratiques.

Cette transformation vise, au travers de nouveaux usages, à s'approprier rapidement et dans les meilleures conditions les technologies émergentes, pour générer des ruptures dans les pratiques, les organisations et les modes de travail ou d'action.

La donnée numérique est au centre de ces enjeux. Il est nécessaire d'apprendre à mieux la traiter, mieux la sécuriser au niveau national et la partager au bénéfice de l'action globale des armées en opérations et dans le fonctionnement quotidien du ministère des Armées.

En tant que pilier de la confiance, l'identité numérique est un autre enjeu d'importance pour l'État. Son déploiement, sa sécurisation et sa viabilisation sont en effet indispensables à la généralisation des démarches dématérialisées, tant dans les relations commerciales que dans la relation du citoyen à une administration moderne.

Toujours dans le cadre de l'ambition numérique du ministère, la souveraineté numérique s'exprime par la volonté du ministère d'amplifier les capacités de développements rapides. Ces capacités favoriseront l'emploi de logiciels aux sources libres, constituant un puissant facteur d'indépendance et d'agilité dans la mise à disposition de nouveaux services.

Au-delà de la technologie, il s'agit aussi de s'attacher de nouveaux talents d'innovateurs et d'injecter agilité et attractivité dans les métiers numériques du ministère. Dans le courant de l'année 2018, la

(1) http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf
(2) http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf (chap 7.C)
(3) https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/
(4) http://discours.vie-publique.fr/notices/163003632.html
(5) https://www.defense.gouv.fr/dgris/presentation/evenements/revue-strategique-de-defense-et-de-securite-nationale-2017
(6) https://www.defense.gouv.fr/actualites/articles/innovation-numerique-le-ministere-poursuit-sa-transformation

création de la DGNUM [7] comme chef d'orchestre de cette dynamique permettra d'accélérer et de structurer cette démarche de profonde modernisation et de transformation menée en cohérence avec celle initiée en interministériel au sein d'Action Publique 2022 [8]. Trois objectifs stratégiques de performance structurent cette démarche :

- Garantir la supériorité opérationnelle et la maîtrise de l'information sur les théâtres d'opérations ;
- Renforcer l'efficience des soutiens et faciliter le quotidien des personnels ;
- Améliorer la relation au citoyen et l'attractivité du ministère.

## L'enjeu de la connaissance : anticipation et renseignement

Action aux canaux multiples, l'anticipation repose notamment sur le renseignement, tant dans sa finalité d'action que dans son acception de veille stratégique. Sur le long terme, il s'agit en effet d'anticiper les évolutions et les tendances pour permettre à la France de décider et d'agir de manière autonome et souveraine. C'est le rôle de la veille stratégique conduite au sein du ministère des Armées.

Sur le temps plus court et potentiellement à fin d'action, le besoin en renseignement est déterminant. Théoriquement, une ligne de séparation existe entre le renseignement d'origine cyber (ROC) et le renseignement d'intérêt cyber (RIC). Si le ROC est défini comme le renseignement provenant de sources cybernétiques (sources ouvertes, essentiellement mais pas toujours de l'Internet, recherches informatiques et investigations de supports numériques comme les disques durs, les clés USB, les téléphones, les tablettes ou l'électronique des systèmes d'armes…), le RIC a quant à lui pour vocation d'apporter à la chaîne de commandement opérationnel de la cyberdéfense militaire les informations dont la connaissance et la compréhension sont nécessaires pour opérer en sécurité dans le cyberespace. Il vise à évaluer la menace cyber qui pèse sur les forces en opérations et à exploiter les opportunités dans le camp adverse.

La capacité à échanger le renseignement est essentielle, tant à l'intérieur du ministère qu'avec nos alliés, tout comme celle d'orienter les recherches. Ce processus a lieu autour du cycle classique du renseignement : orientation, recherche et acquisition, exploitation, diffusion.

## La capacité d'action

En dernier ressort, la souveraineté doit pouvoir être garantie par une capacité d'action. Deux impératifs sont corollaires de la capacité d'action : la résilience des systèmes des armées et la possession d'options défensives comme offensives.

Un certain zèle peut conduire à confondre la résilience nécessaire à la souveraineté avec une indépendance ou une autonomie totale des moyens. Dans un système économique mondialisé, cette orientation n'apparaît pas pertinente, les armées n'étant pas en mesure de contrôler de bout en bout l'autonomie de leur production en électronique et en informatique. Partageant sur ce point la position d'autres partenaires, le choix est fait de ne fortement sécuriser que ce qui est vital au sein d'un environnement qu'on estime peu sûr. Les armées n'ont ainsi besoin de maîtriser en propre que quelques composants bien précis pour pouvoir sécuriser un ensemble composé de briques peu fiables. Tout d'abord, il s'agit d'avoir des outils de cryptographie souverains pour assurer l'intégrité et la confidentialité des données. Ensuite, la maîtrise des réseaux nécessite notamment la possession de sondes de détection entièrement fiables et maîtrisées, afin de garantir la disponibilité des données. Enfin, il faut des algorithmes nationaux pour assurer le traitement de ces données.

(7) Direction générale du Numérique et des Systèmes d'Information et de Communication, ex-DGSIC.
(8) https://www.economie.gouv.fr/lancement-programme-action-publique-2022

La garantie de disposer des moyens présentés répond aux besoins fondamentaux des armées. En effet, l'absence de certification systématique des matériels et des logiciels est palliée par le chiffrement et la disponibilité de service. Par ailleurs, bien que les armées ne soient pas autonomes en matériels et en logiciels, elles peuvent être considérées comme indépendantes par la diversité des sources d'approvisionnements et de fabrications, et l'emploi de plusieurs réseaux protégés et physiquement séparés.

En outre, croire que les composants ou les logiciels pourraient tous être nationaux ou européens est une illusion. Cet effort serait inutile car, même développés en propre, les produits numériques ne pourront jamais être considérés comme parfaitement fiables. De plus, leur maintien à jour et en condition de sécurité est bien souvent un défi coûteux, rendant les logiciels propriétaires non nationaux très attractifs.

Enfin, le développement des *data sciences* et du *machine learning* crée un nouveau besoin : posséder des ensembles, ou *sets* nationaux de données labellisées pour entraîner ou évaluer les algorithmes [9]. Par exemple, dans un environnement de plus en plus dépendant du renseignement en source ouverte et des moteurs de recherche, il est important de pouvoir évaluer la fiabilité et les biais des moteurs publics. Ce besoin dépasse le cadre strict des armées et interroge sur la confiance à accorder à des algorithmes non publics. La validation des algorithmes privés par des *sets* secrets de données gérés par des organismes de contrôle publics pourrait répondre à ce besoin de certification.

> « L'enjeu considérable que représente la menace cyber appelle un renforcement substantiel à la fois des moyens défensifs et offensifs de la France. La capacité de détection et d'attribution des attaques, qui repose sur l'acquisition de renseignement d'origine humaine aussi bien que technique, en sera un élément-clé. »
>
> (*Revue stratégique*, §299, octobre 2017)

Le second aspect de la capacité d'action est de conserver une force de frappe défensive ou offensive prête à servir. Un cyberespace omniprésent est en effet un enjeu stratégique tant civil que militaire. La communauté internationale éprouve d'ailleurs des difficultés à faire émerger un cadre juridique international adapté. Outre les grandes puissances et certaines puissances moyennes, qui disposent de l'ensemble des capacités d'actions cyber et qui, dans le cadre de concurrences politique ou économique, peuvent conduire des actions de renseignement inamicales, de nombreuses nations ou organisations structurées peuvent conduire des opérations dépassant le stade de l'espionnage. Les groupes activistes doivent également être pris en compte, ainsi que ceux liés au terrorisme international et aux différentes formes de nationalismes.

Le cyberespace est devenu un champ de confrontation à part entière. Les armées doivent disposer des capacités de maîtrise et d'action dans ce milieu. De même, l'État, au travers de ses institutions, doit maintenir son fonctionnement, les activités d'importance vitale, la sécurité et l'activité économique face à ces menaces cybernétiques. Elles peuvent être regroupées en trois familles : celles ciblant directement les informations, celles visant les systèmes d'information eux-mêmes et celles qui passent par le cyberespace pour viser des objectifs physiques (équipements et installations critiques, etc.).

(9) Les modèles supervisés sont entraînés avec des données dont les résultats attendus, « labels », ont été complétés auparavant (manuellement ou par des automates). Les biais de la labellisation du set d'entraînement se retrouvent ainsi « gravés » dans le fonctionnement de l'algorithme.

Or, dans le cyberespace, les notions de preuve, d'imputabilité des actions ou attributions sont plus complexes à faire émerger. Cela modifie le rapport de force classique entre l'attaquant et le défenseur : l'avantage relatif qu'a l'attaquant est renforcé par la prolifération des technologies d'attaque, comme par exemple Wannacry [10]. L'action dans le cyberespace est délicate à conduire, et la France se veut moteur dans la construction d'un cadre international mettant en place des processus, pour les volets tant défensif qu'offensif.

Le ministère des Armées a un rôle bien précis pour ce qui concerne la souveraineté numérique nationale : garantir à la fois un haut niveau de performance dans toutes ses composantes en bénéficiant de la révolution numérique, mais aussi se déployer et combattre dans ce nouvel espace. Pour garantir de façon pérenne leur réussite, les armées sont en pleine transformation digitale, tant de leurs processus que de leurs équipements. La création du COMCYBER puis de la DGNUM dans le courant de l'année 2018 démontre que le ministère a adapté son organisation pour répondre aux défis posés par l'espace numérique, milieu évolutif, compressé et fait d'immédiateté, qui interroge l'ensemble de nos modèles.

(10) Logiciel malveillant de type ransomware auto-répliquant.