Introduction à ce numéro hors-série "Cybersécurité"

Par Martine Cuttier

Les dernières décennies du 20e siècle ont vu émerger et se développer les systèmes d'information et de communication. Ils s'imposent aujourd'hui dans tous les secteurs des sociétés, développées ou non, et révolutionnent les modes de vie et de relation. Plus complexes, les sociétés développées sont potentiellement aussi les plus vulnérables. Si les activités permises par le cyberespace améliorent nos vies à plus d'un égard, ce champ est également un nouveau lieu de conflictualité et de malveillance qui met en cause la sécurité, individuelle et collective. La souveraineté des États s'en trouve affectée, et avec elle les relations internationales et les questions de défense. Au-delà, c'est la société tout entière qui est exposée au risque de paralysie ou de désorganisation sectorielle.*

Les différents types de menaces, les attaques avérées, leurs effets d'ores et déjà observables et les moyens d'y parer ont conduit à l'émergence d'un champ d'études et de recherche à part entière. La France ne fait pas exception, et ceux qui traitent des questions soulevées forment une petite communauté dont les publications et interventions se multiplient depuis 2012. Traitant de sujets importants, elle mérite d'être écoutée et entendue. C'est la raison pour laquelle la revue ***Res Militaris*** a cru bon de consacrer à la cybersécurité un premier numéro hors-série.

Celui-ci est entièrement francophone. Il comporte 15 contributions, dont les auteurs émanent pour moitié de la communauté militaire – jusqu'au plus haut niveau, puisqu'on y note les signatures (au bas d'un article) du général **Denis Mercier**, actuel Chef d'état-major de l'armée de l'Air, et (pour la préface) du vice-amiral **Arnaud Coustillière**, coordinateur "Cyber" à l'État-Major des Armées. Conformément à la vocation de la revue, la Défense occupe donc une place de choix, au travers des hommes et des thèmes, dans ce numéro. Mais des thématiques plus larges y apparaissent dans des articles signés d'auteurs jeunes ou confirmés, venant d'horizons divers.

De quoi parle-t-on ? L'un des articles pose la question (difficile) de la définition : le cyberespace est-il un environnement, un domaine, un milieu ou un moyen ? Les autres tournent autour des origines, des techniques, des atouts que promet mais surtout des vulnérabilités que recèle le cyberespace, des parades, et de la manière dont la conflictualité, la guerre et les sociétés s'en trouvent affectées. Les réponses convergent largement.

---

* *Cf*. Martine Cuttier, *Cyberespace et sécurité globale : enjeux stratégiques*, Paris, CFRS, juillet 2015.

Le texte d'ouverture, signé de **Claude Imbert**, replace numérique et algorithmes dans le temps long en évoquant leur antécédent historique commun : la "roue pascaline", machine à calculer dédiée à des opérations arithmétiques. L'auteure montre comment, reprise et prolongée par les grands scientifiques du 17e au 19e siècle, la démarche de Pascal débouche au 20e sur la transcription algorithmique et la puissance du numérique, lesquelles s'intègrent dans le développement des mathématiques depuis l'Antiquité.

Le second article est d'un informaticien et chercheur, **Philippe Truillet**. Il s'y s'intéresse à Internet, "réseau des réseaux", qui s'impose au fil du temps comme "*un standard incontournable, présent sur quasiment tous les réseaux physiques permettant l'acheminement d'informations*". Il en mentionne brièvement l'origine : le réseau ARPANET qui en 1969 permit d'établir la première communication à distance entre ordinateurs – ceux des chercheurs de l'université de Californie à Los Angeles et de Stanford. Doug Engelbart, inventeur de la souris et précurseur des systèmes hypertextes, en a le premier compris toutes les potentialités : l'émergence d'un nouveau marché de produits et de services aux possibilités infinies. Ph. Truillet présente ensuite l'architecture du réseau, montre que sa structuration permet d'appréhender ses forces comme ses faiblesses, et décortique le schéma des cyberattaques, résumant les types de menaces, leurs auteurs et les ripostes mises en place, entre autres, par l'État. Au vu de la complexité du phénomène "cyber", il invite pour finir à promouvoir une véritable culture informatique dans la société, et à décloisonner les disciplines concernées : "*un informaticien ne peut plus ignorer les textes de loi régissant l'usage des réseaux et les sanctions auxquelles il s'expose, pas plus qu'un juriste ne peut désormais ignorer le mode de fonctionnement 'basique' des systèmes informatiques*".

À la suite, le général de gendarmerie (2S) **Marc Watin-Augouard** analyse le concept de *continuum défense-sécurité* appliqué au cyberespace. Formalisé en France dès 1992, peu ou prou délaissé par le *Livre Blanc* de 1994, il est clairement affirmé dans ceux de 2008 et 2013. À compter de 2008, les livres blancs, jusque-là "de la défense nationale" ajoutent à leur titre le vocable "sécurité", et peu après le SGDN devient SGDSN. La même année (2009) est créée en son sein l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le concept de continuum défense-sécurité est enfin adopté par l'Union européenne lors de la mise en œuvre du traité de Lisbonne (2009), puis par l'OTAN (2010). L'auteur poursuit sa présentation par une précieuse vue d'ensemble des questions posées, des problèmes à résoudre, et des voies et moyens, d'ores et déjà en place, de la coopération interministérielle en la matière en France.

Comme les autres contributeurs, **Aymeric Bonnemaison** insiste sur une réalité qui s'impose à tous aujourd'hui : "*le cyber est déjà de tous les conflits.* […] *Il permet des raids discrets dans la profondeur d'un dispositif stratégique. Il s'insère dans les guerres classiques*". Et d'analyser comment le cyberespace est devenu un élément de la guerre dans ses trois couches constitutives : *physique* (infrastructures, stockage de données), *logicielle* (codes et programmes) et *sémantique* (contenus de sens). Dans cette dernière, "*le cyber est devenu l'acteur majeur de la guerre de l'information*", lieu de la provocation, de la

radicalisation mais aussi de la terreur et de la fascination, bien illustré par l'usage qu'en font les *djihadistes* et particulièrement *Daech*. Le colonel Bonnemaison montre ensuite que la bataille logicielle est engagée, dans le silence et le secret. C'est par exemple ce qu'on a vu avec l'opération qui a permis, grâce au virus *Stuxnet*, de ralentir à distance et pour un temps le programme iranien d'accès à l'arme nucléaire. Enfin, la couche physique n'échappe pas aux batailles. En 2008, lors de la guerre de Géorgie, le cyber a investi le champ de bataille et provoqué la défaite géorgienne. En Crimée et en Ukraine, la maîtrise du combat cyberélectronique confirme la tendance, déjà entrevue chez les Russes, à mener des attaques simultanées dans les trois couches. L'auteur note pour finir que si cette forme de combat change peu les principes de la guerre, elle s'ajoute de manière significative, par un nouveau mode d'action, aux formes plus anciennes.

Les trois armées répondent à ces nouvelles réalités, et particulièrement l'armée de l'Air. Le **général Mercier** passe en revue les diverses manières dont les forces aériennes françaises conçoivent et utilisent la dimension "cyber". Au-delà d'analogies de forme entre opérations Air et Cyber, il pointe des différences et des complémentarités entre elles, et conclut à la nécessaire synergie des deux domaines, fortement interdépendants et interactifs, au sein du système de combat aérien futur.

Il est suivi dans cette voie par un spécialiste civil de la "troisième dimension", connu pour ses travaux d'historien de l'aviation : **Gaëtan Sciacco**, qui pose la question un peu provocante d'un hypothétique "*cyber Pearl Harbor*" dont l'armée de l'Air aurait du mal à se relever. Il commence par décrire une mission de combat en appui tactique pour mieux illustrer ce que sont les guerres de type *info-centré*, devenues le modèle d'engagement des forces depuis la guerre du Golfe de 1991. Dans cette très vivante évocation, il n'oublie aucune des unités ou fonctions aériennes impliquées dans ce processus où les logiciels sont en première ligne, et sont autant de points de vulnérabilité. Ayant décliné la gamme étendue des menaces venues de la cybersphère, il évoque le plan stratégique quinquennal "*Unis pour faire face*", qui pour y parer conjugue programmes de formation et renforcement des structures d'expertise cyberdéfense. Il pose pour finir une question qui a le mérite d'être sans détour : "*à l'heure où l'avion piloté est remis en cause, entre autres par le drone, se pourrait-il que dans un avenir plus ou moins proche, les aviateurs cèdent du terrain dans la troisième dimension, mais compensent ce phénomène par le développement d'un ascendant plus grand sur le monde spatial et surtout sur le cyberespace*" ?

La transition est toute trouvée pour introduire l'article suivant, signé de **Panpi Etcheverry**, qui compare l'impact de ces deux armes nouvelles que sont le drone et le cyber. Il en tire l'idée que l'un et l'autre s'inscrivent dans un même mouvement civilisationnel et de mutation de la guerre marqué par l'avènement de l'"infosphère", source de "complexité stratégique". Il pointe des risques majeurs de déstabilisation si (comme c'est le cas aux États-Unis aujourd'hui) leur usage n'est pas sous-tendu par une réflexion stratégique d'ensemble, et conclut : "*Les drones comme le cyber sont donc au cœur de mutations considérables dont les conséquences ne sont pas toutes mesurables*

aujourd'hui. Ils interrogent les normes et les pratiques en vigueur jusqu'à maintenant, le rôle de l'État et du secteur privé, la portée de la notion de souveraineté et de frontière, et peuvent laisser à penser qu'ils constituent des armes ultimes. Pour autant, il n'en est rien".

Le général (2S) **François Chauvancy** consacre la totalité de sa contribution à la question de savoir s'il n'y aurait pas avantage à considérer que le cyberespace est un champ de bataille des idéologies avant d'être celui des technologies. Il appuie sa démonstration sur les attentats du 7 janvier 2015 et la cyberattaque contre *TV5 Monde*. "*La technique semble bien avoir permis le réveil des idéologies ; celles-ci* […] *ne se résument pas au seul péril djihadiste, mais sous-tendent aussi les stratégies d'influence d'États comme la Russie ou la Chine*". Le général Chauvancy insiste sur le rôle cardinal de l'influence, et en tire la conséquence : "*Face à ces nouvelles guerres idéologiques, la nécessité pour nous est d'agir en stratèges. L'objectif doit être défini dans une approche à long terme : par exemple, à l'extérieur de nos frontières ou sur le territoire national, les djihadistes doivent être convaincus de notre volonté de les éradiquer, et défaits. La guerre implique et affecte aussi bien les corps que les esprits. Une prise de conscience est en cours, et il faut s'en féliciter*".

Dans leur très courte contribution, **Thomas Flichy de la Neuville** et **Olivier Hanne** ont justement choisi le cas de *Daech*, dont les succès cybernétiques sont en partie liés à son savoir-faire médiatique. Ce savoir-faire est mis au service du recrutement de nouveaux membres et de campagnes de terreur contre ses opposants en Irak et en Syrie. Au-delà, cette terreur soigneusement médiatisée vise les populations civiles de la région, mais encore les opinions publiques occidentales. Outre ces effets recherchés, les auteurs passent en revue les moyens techniques mis en œuvre par l'"État islamique" et, de manière plus originale, les limites de son action.

Jonathan Rétif s'intéresse, quant à lui, à la simulation – notamment aux jeux vidéo utilisés dans la formation des acteurs et concepteurs militaires. Il s'interroge quant aux effets que ces simulations plus ou moins réalistes produisent sur les représentations, voire sur les constructions idéologiques, des personnels directement concernés, et par ricochet sur celles qui président à la formulation des politiques de sécurité nationale. Autrement dit : "*quels pourraient être le potentiel caché et les implications de la simulation à vocation militaire*" *?* Il constate qu'il reste "*à approfondir les liens qui émergent entre les constats précédents et les objectifs des acteurs qui les mobilisent (États, complexes militaro-industriels, industries du jeu vidéo) tout en replaçant ces relations dans le contexte contemporain des relations internationales* […]. *Cet axe d'étude peut également contribuer à la dynamique actuelle de la recherche : celle qui explore les pistes susceptibles de mener à une maîtrise du cyber par l'identification des vulnérabilités qu'il engendre et de nouveaux moyens d'action sécuritaire pour y parer*".

On a gardé pour la fin les articles qui ouvrent la focale et débordent la dimension militaire. Le premier est signé d'**Olivier Kempf**, qui y fait œuvre de sociologue en examinant comment le cyberespace transforme le rôle et le statut de groupes marginaux et de significations expressives excentrées par rapport à la culture dominante des sociétés.

Ces marges sont désormais promises à perdre de leur marginalité, et à devenir à titre normal l'un des moteurs du changement politique, culturel et social : "*la marge d'antan supposait une certaine stabilité, une déviance continue par rapport à une position établie. La marge nouvelle apparaît* […] *non plus comme une séparation ou un extrême, mais comme le* front marchant *de l'évolution sociale*".

Vient ensuite **Emmanuel Meneut**, qui au travers de deux exemples récents – une panne électrique géante au Brésil (2009) et le vol de données par des pirates anonymes au détriment de *Sony Pictures Entertainment* (2014) – s'interroge sur le rôle des militaires "*lorsque la légitimité de l'État est mise en cause par une cyberattaque d'origine incertaine sur une infrastructure civile*" sensible, publique ou privée. Il montre que les retombées politiques internes et externes en sont peu négligeables, et que la parade passe par un couplage État-entreprise, maillon critique de la sécurisation. Or, si l'État est allant en la matière, les entreprises (comme aux États-Unis) le sont parfois beaucoup moins…

Le troisième article de cette catégorie est de **Jean-Paul Mazoyer**, cadre dirigeant du Crédit Agricole, qui s'intéresse à la cybersécurité à l'heure de la "transformation digitale" dans le monde de la banque et de l'entreprise. Selon lui, les remèdes aux vulnérabilités nouvelles nées dans le cyberespace sont à rechercher conjointement du côté des technologies, des compétences nouvelles à s'approprier (notamment et surtout la cryptographie), et des modalités de contrôle. Il conclut : "*La démonstration est faite que la transformation digitale de l'entreprise doit embarquer d'emblée la dimension sécuritaire sur tous les axes : conception des produits, construction et pilotage des infrastructures, formation et sensibilisation, gestion de crise, modalités de contrôle. Nouveaux métiers, nouvelles approches, nouvelle mentalité. Et puisque la somme des transformations numériques des entreprises se traduit par une transformation numérique de la société dans son ensemble, l'État (superviseurs) a un rôle à jouer selon des modalités à réinventer*".

Ce numéro spécial se clôt par la contribution d'**Yves Auffret**, doctorant et officier-instructeur sous contrat à l'École de l'Air, qui confronte les théories des relations internationales à l'objet opaque, foisonnant et fluide, aussi décentralisé que mal défini, qu'est le cyberespace. Au terme d'une discussion (menée selon une approche constructiviste et systémique) des aspects discursifs et normatifs de la question, il le voit comme un objet construit, catalyseur d'anarchie dans les relations internationales.

Si, comme on le souhaite, ce premier "hors-série" a convaincu les lecteurs de ***Res Militaris*** de l'importance et de l'intérêt critiques de la cybersécurité, il aura rempli l'office qui lui était assigné.

Bonne lecture !

Martine Cuttier