Cyber Défense
Introduction

Didier Danet[*], Centre de recherche des écoles de Saint-Cyr Coëtquidan, Pôle « Mutation des conflits »

Rien de plus banal que de constater la dépendance actuelle des entreprises, des administrations et des armées à l'égard de techniques ou de services informationnels qui étaient encore embryonnaires il y a moins de vingt ans. Dans ce laps de temps plus que réduit, les progrès des sciences et des techniques ont bouleversé les structures, les stratégies, les modes d'action et les comportements de l'ensemble des acteurs, civils aussi bien que militaires. Ils ont engendré de nouvelles menaces en même temps qu'ils ont ouvert de nouvelles opportunités. Plus encore, le foisonnement et la convergence des découvertes et des innovations intervenues dans de nombreux domaines (électronique, intelligence artificielle, énergie, nano-technologies...) conduisent à une transformation globale de la société, la « numérisation », dont les définitions peinent à embrasser l'ensemble des dimensions et des applications.

Pour ce qui concerne les forces armées, lesquelles participent activement de cette transformation, la « numérisation de l'espace de bataille » (NEB) peut s'entendre dans un sens restreint qui renvoie à la volonté de l'armée de Terre de collecter, traiter et diffuser en temps réel les informations nécessaires aux différents échelons de commandement sur le champ de bataille. Elle s'analyse alors comme la mise en place d'un artefact technique (un internet du champ de bataille composé de systèmes d'information à plusieurs niveaux) qui supporte un ensemble de systèmes d'analyse des données et d'aide à la décision susceptibles d'apporter aux chefs militaires un avantage décisif sur leurs adversaires. Elle s'inscrit dans la logique du « Network Centric Warfare » où le succès repose sur la combinaison d'une organisation réticulaire, reconfigurable en tant que de besoin et irriguée par un

[*] Didier Danet est responsable du pôle « Mutation des conflits » du Centre de recherche des écoles de Saint-Cyr Coëtquidan. Il est également directeur du Mastère Spécialisé « Opérations et gestion des crises en cyber défense ».

flux d'informations suffisamment riche pour atténuer dans des proportions inédites jusqu'ici le brouillard de la guerre et les frictions du champ de bataille. La question centrale est alors de rechercher les moyens de tirer le meilleur parti de cette capacité inédite de traitement de l'information en l'intégrant dans une structure et des procédures qui ont été conçues antérieurement.

De manière plus profonde, la « numérisation » est un processus de transformation globale, un « Mega Trend » ou une « Ultra-Force », qui modifie les paramètres fondamentaux de la pensée et de l'action militaires :

- L'espace et le temps : la numérisation offre des possibilités d'action qui s'affranchissent dans certains cas des distances et du temps. Combinée avec les capacités plus traditionnelles de la guerre électronique, les actions de lutte informatique offensive permettent d'exercer certaines formes de coercition sans que leur auteur ne soit contraint par l'éloignement ou par des délais de mise en œuvre.
- Dans l'espace cinétique, la numérisation a apporté des gains déterminants à la précision des actions, en particulier dans la mise en œuvre du feu qu'il s'agisse par exemple de l'automatisation conférée aux batteries anti-missiles du système Phalanx ou de l'usage des drones pour frapper des cibles particulières.
- Enfin, la croissance exponentielle des capteurs combinée avec des capacités de traitement de l'information et d'aide à la décision révolutionnent la connaissance de l'environnement du champ de bataille aussi bien que la manière dont les chefs militaires de tous niveaux seront amenés à réfléchir, à prendre les décisions et à interagir avec leurs supérieurs et leurs subordonnés.

La numérisation est donc un processus global dont l'ensemble des dimensions ou des effets ne sont pas entièrement planifiés et conduits de manière délibérée. Il ne s'agit pas seulement de rechercher les moyens de « greffer » au mieux un système technique nouveau sur une institution existante en suivant les processus de planification conformes à la logique et aux procédures bureaucratiques. La numérisation fait bien évidemment l'objet d'un pilotage par le haut, comme le montre l'exemple remarquable du système Scorpion, lequel donne à l'armée de Terre les moyens d'une ambition : le combat collaboratif. Mais, de manière tout aussi évidente, elle transforme « par le bas » le système socio-technique qu'est l'organisation militaire, le rythme et la nature des innovations, leur niveau d'acceptation individuelle et sociale ou leurs effets sur les comportements organisationnels étant assez largement dépendants de facteurs extérieurs à la volonté des organes chargés du pilotage de la « NEB ».

Ces deux acceptions du concept de « numérisation » ne sont pas exclusives l'une de l'autre. Au contraire, elles sont porteuses de questions ou d'enjeux qui sont connexes et complémentaires. L'article de Clotilde Bômont identifie ceux de ces enjeux qui sont liés à la numérisation en tant que projet de transformation piloté par les forces armées. Elle montre en particulier que le progrès technique (le « Cloud Computing » en l'espèce) soulève une interrogation liée à la triple concentration qui en résulte (des infrastructures / des applications / des données) et qui suppose de développer une véritable « stratégie du Cloud militaire ». La « Cloudification » trouve son origine dans un ensemble de questions techniques liées à la manière de stocker les données. Mais, elle ne se limite pas à la seule dimension technique dans la mesure où elle modifie les termes du débat relatif aux structures militaires optimales, notamment parce qu'elle renforce positivement l'intérêt pour des structures militaires réticulaires dont la supériorité résulte précisément d'une capacité supérieure d'acquisition et de traitement de l'information. On s'attachera en particulier à la proposition formulée par l'auteure d'une grille d'évaluation du périmètre stratégique susceptible de guider les choix structurants en matière de « Cloud Défense ». La grille proposée est encore provisoire puisqu'elle fait l'objet d'une thèse financée par la Direction Générale des Relations Internationales et de la Stratégie du ministère des Armées. En écho à la réflexion de Clotilde Bômont, Stéphane Taillat et Amaël Cattaruzza proposent quant à eux une analyse de la numérisation comme processus dans lequel interagissent des volontés et des forces qui leur échappent pour produire un nouvel état du système socio-technique dont les propriétés et les caractéristiques échappent en plus ou moins grande part à ceux qui l'ont initiée. Il s'agit de dépasser la quête d'une hypothétique « One Best Way » que les armées se devraient de suivre pour réaliser la « greffe » du numérique et obtenir les résultats uniformément promis à ceux qui acceptent de s'engager dans cette voie. Les auteurs soulignent à juste titre que la numérisation, comme toutes les innovations majeures adoptées par l'institution militaire, fait apparaître des propriétés émergentes du système et des comportements contingents des acteurs. Il s'agit donc de reconnaître la part d'indétermination qui est associée à l'implantation du numérique dans les armées. Tout écart au plan de déploiement voulu par les pilotes de la « NEB » n'est pas nécessairement une anomalie qu'il conviendrait de corriger au plus vite et sans faiblesse. Le principe de tels écart doit être accepté comme la conséquence nécessaire de l'existence de propriétés émergentes et de comportements contingents et il convient alors de chercher à en comprendre la pertinence, les enjeux et les effets au regard des concepts et des outils de l'analyse des systèmes socio-techniques, notamment de la théorie de l'acteur-réseau qui est retenue par les auteurs. Cette approche novatrice permet d'aborder la numérisation sous un angle

particulièrement original : analyser le processus à travers ce qui la sous-tend, à savoir l'association de la mise en données de l'objet numérisé et de la mise en réseau des données ainsi constituées. A partir des concepts ainsi développés et en les confrontant à des retours d'expérience très différents, Stéphane Taillat et Amaël Cattaruzza mettent en évidence deux grands types d'apports possibles à la compréhension du processus de numérisation. Le premier tient à la compréhension des comportements organisationnels qui déterminent conjointement avec les caractéristiques techniques des dispositifs implantés la performance globale du nouveau système mis en place. Leur analyse du système CPOF (« Command Post of the Future ») mis en place au sein de la 1ere division de cavalerie américaine lors de la guerre d'Irak (2004) éclaire de manière particulièrement pertinente les débats relatifs aux conséquences possibles des usages effectifs d'un système d'information supposé réduire la complexité du champ de bataille, notamment les précautions à prendre dans le partage des responsabilités entre les différents échelons de commandement. Le second apport de l'analyse porte sur une propriété émergente de la numérisation : la porosité des usages professionnels et privés des objets numériques. Bien que la séparation de ces usages soit un principe cardinal des chartes de sécurité informatiques, leur porosité est un fait social acquis. Or, l'exploitation habile des traces générées par les différents usages peut conduire à produire des informations qui ne sont pas anodines comme l'a montré l'affaire « Strava » au début l'année 2018. Ici encore, les concepts de l'acteur-réseau (ou d'autres grilles théoriques permettant de comprendre les comportements organisationnels) éclairent les faiblesses actuelles des politiques de sécurité informatique, notamment celles des mesures dites « d'hygiène informatique ».

Les deux articles suivants, présentés respectivement par Christine Dugoin-Clément et Saïd Haddad traitent de la dimension sémantique de l'espace numérique. Les deux auteurs abordent deux questions particulièrement disputées mais trop souvent traitées sans les nécessaires cadrages théoriques qui font la richesse particulière des deux textes présentés ici.

A partir d'un travail de terrain mené notamment lors du conflit en Ukraine et qui forme le point de départ de la thèse qu'elle consacre à la question, Christine Dugoin-Clément propose une analyse du concept et des pratiques d'influence qui peuvent être conduites à travers l'espace numérique. En s'appuyant sur la grille de lecture de la dissonance cognitive, elle s'interroge sur deux questions dont l'importance pour les forces armées est tout à fait centrale. La première est celle des ressorts socio-psychologiques qui peuvent expliquer la réussite d'une opération visant à modifier les perceptions et les jugements d'une population en général et des personnels militaires en particulier. Comment évaluer les effets de campagnes insidieuses menées sur les réseaux sociaux ? Un nombre élevé de

« Retweets » dans un laps de temps réduit signifie-t-il à lui seul que le message a été reçu et qu'il a entraîné l'adhésion de ses lecteurs ? Quelles sont les cibles les plus vulnérables face à ces campagnes ? L'hétérogénéité des publics et des usages de l'Internet a-t-elle des conséquences sur la réussite de telles campagnes ? Sur toutes ces interrogations, le travail de Christine Dugoin-Clément apporte des réponses d'autant plus précieuses qu'il se fonde à la fois sur des observations empiriques originales et sur une réflexion théorique rigoureuse. La seconde question abordée dans l'article est celle de l'application des résultats obtenus au cas particulier des forces armées. En quoi celles-ci peuvent-elles être la cible d'opérations d'influence ? Les personnels militaires sont-ils plus que d'autres sensibles à certaines formes d'action psychologique ? Quelles formes ces actions pourraient-elles prendre avant et pendant un conflit ? Quelles mesures pourraient être mises en place pour prévenir l'impact négatif de ces opérations ? Dans des débats où règnent le plus souvent les fantasmes ou les imprécations, le cadre théorique et les terrains qui sont mobilisés par Christine Dugoin-Clément permettent de construire une politique rationnelle et efficace permettant de comprendre, de mesurer et de contrer les politiques d'influence menées à travers l'espace numérique. L'article de Saïd Haddad porte quant à lui sur la construction du discours politique sur le cyber-terrorisme. On sait qu'en dépit de la très grande inconsistance, voire de la vacuité du concept et de l'insignifiance des effets réellement obtenus par les cyber attaques imputées à des organisations terroristes, le terme a rencontré un très grand succès dans le monde politico-médiatique. Il était donc essentiel de chercher à comprendre la logique à l'œuvre dans la construction et le déploiement de ce discours. L'article mobilise le cadre théorique particulièrement pertinent et éclairant qui est celui développé par l'école de Copenhague. Ce dernier permet de comprendre notamment comment des effets politiques substantiels peuvent être obtenus par l'instauration d'une menace intersubjective suffisamment saillante. En prenant appui sur les trois concepts fondamentaux de ce cadre théorique (amplification de la menace / mobilisation des individus / technification de l'analyse) et en les analysant dans le contexte du défacement de TV5 Monde, l'auteur montre comment une cyber-attaque de conception rudimentaire et aux effets très circonscrits a pu donner naissance à un discours et des mesures sécuritaires qui ont fait de la lutte contre le cyber-terrorisme une priorité des pouvoirs publics.

L'article qui conclut cette livraison de *Dynamiques Internationales* propose une réflexion sur le devenir de la conflictualité dans l'espace numérique. Ce dernier est maintenant une donnée évidente de toute réflexion sur les processus de coopération et de compétition qui s'y déroulent. Après une période d'émergence et de montée en puissance, la réflexion sur le « Cyber Warfare » est aujourd'hui entrée dans une phase de relative maturité où, la lumière aveuglante de la novation technique s'atténuant quelque peu, les premières interrogations qui lui étaient directement liées sont mieux maîtrisées, n'occupent plus nécessairement le devant de la scène et font l'objet d'un réinvestissement par les sciences sociales et politiques. On songe par exemple à la littérature relative à l'attribution des cyber-attaques. Dans une première phase, cette littérature a fait la part belle à la dimension technique de l'attribution et à la possibilité (ou à l'impossibilité) pour les experts de démasquer l'auteur de cyber attaques à des traces plus ou moins convaincantes qu'il aurait laissées derrière lui : heure de la préparation des attaques, maîtrise de la langue utilisée pour le codage, valeur ajoutée de l'attaquant par rapport aux outils disponibles en « libre service » sur Internet… Dans un passé encore récent, une entreprise américaine proposait de créer à Genève une commission d'experts internationaux qui serait chargée de se prononcer scientifiquement et « en toute indépendance » sur l'attribution des attaques. On ne saurait dire si cette proposition relève du cynisme mercantile ou de la naïveté politique tant elle semble méconnaître le caractère intrinsèquement politique de l'acte consistant pour un Etat à imputer à un autre l'initiative d'une attaque et à justifier ainsi une série de réponses plus ou moins coercitives à son encontre. De même, la perspective d'un bouleversement de l'ordre mondial du fait de l'asymétrie supposée des acteurs dans le cyber espace s'est évanouie. La puissance numérique apparaît aujourd'hui directement liée aux facteurs habituels de la puissance politique, économique ou militaire. Les Etats les plus avancés techniquement, ceux qui disposent des ressources humaines les plus qualifiées, des capacités industrielles les plus importantes ou des moyens budgétaires les plus abondants sont naturellement ceux qui disposent des positions de force dans l'espace numérique comme dans l'espace physique. Le fantasme de l'étudiant qui défie les pays les plus puissants du fond de sa chambre à la cité universitaire s'est dissipé pour revenir à une analyse relativement classique de la sociologie des relations internationales et des acteurs de ces relations. Si elles ne disparaissent pas complètement et si elles demeurent d'actualité, les interrogations initiales s'orientent désormais plutôt vers les usages possibles du numérique au sein de l'action globale des forces. Comment en particulier articuler numérique et cinétique dans une politique de coercition ? Comment intégrer pleinement les menaces et les opportunités résultant de l'interconnexion généralisée des systèmes d'information ? Comment faire en sorte que les unités et

les personnels responsables des opérations numériques ne se trouvent pas enfermés dans une technique qui deviendrait une « boîte noire » pour les chefs militaires ? Ici encore, les théories, concepts et outils des sciences sociales permettent d'apporter des éclairages complémentaires des sciences de l'ingénieur. L'article propose ainsi de confronter les promesses de performance technique du programme Scorpion avec la grille de lecture tirée de la théorie du comportement organisationnel. Il ne s'agit bien évidemment pas de nier le caractère remarquable, probablement inédit, des avancées réalisées grâce au système d'information développé dans le cadre de ce programme. Mais, il s'agit de souligner qu'à côté des facteurs techniques de performance, la réussite d'un programme dépend également de facteurs socio-techniques qui doivent s'apprécier au triple niveau de l'individu qui s'approprie plus ou moins bien le nouvel équipement, des groupes qui se trouvent impactés dans leur organisation et leur fonctionnement et de l'organisation elle-même dont la culture dominante peut être remise en cause par des innovations de rupture.