ECOLE DE GUERRE

Promotion Général *GALLOIS*

2016 -2017

En quoi un monde de plus en plus connecté nous conduit-il à repenser nos C2 ?

par le lieutenant-colonel Michaël Alcantara

Sous la direction du
Lieutenant-colonel, Docteur Olivier Entraygues,
Chercheur à l'Institut de recherche stratégique
de l'Ecole militaire (IRSEM)

Résumé

A l'instar de l'ensemble de la société, les organisations militaires sont irrémédiablement concernées par l'omniprésence d'une information qui est devenue tout à la fois centrale et de plus en plus difficile à gérer de par l'interconnexion sans cesse accrue des différents réseaux.

Les évolutions technologiques en matière de communications et de traitement de l'information ont eu d'indéniables apports opératifs. Elles ont néanmoins tout autant mené à des mutations difficilement conciliables avec la conception traditionnelle du C2, entendu désormais comme « commandement et conduite » des opérations. En effet, outre les nécessaires métamorphoses des systèmes hiérarchiques, la place prépondérante des réseaux et l'instantanéité induite des échanges ont conduit à une transformation des perceptions du temps et de l'espace. Dans le même temps, de nouveaux acteurs ont fait leur apparition dans l'espace d'affrontements, directement sur les champs de bataille qui, de surcroît, sont de plus en plus numérisés et mis en réseaux. Parallèlement, le décloisonnement des échanges d'informations ont conduit à une compression des niveaux de conception et de conduite des opérations.

Dès lors, face aux nouvelles menaces qui trouvent consistance dans le cyberespace et eu égard à l'enjeu croissant de la supériorité informationnelle, les C2 doivent se transformer à dessein de garantir une prise de décision toujours plus réactive et une exécution de la manœuvre militaire toujours plus efficace, tandis que les considérations juridiques et éthiques sont de plus en plus prégnantes.

Abstract

As with the rest of society, the military organizations are irremediably affected by the ubiquity of information. Information has become pivotal and ever harder to manage due to the relentless increasing in network interconnections.

The technological developments communications and information management systems have indisputably improved operations; however, these have also created some effects that are hardly compatible with the traditional conception of "Command and Control, or C2. As a matter of fact, besides the mandatory changes to the hierarchical structures, the primacy of the networks and the related instantaneity of the exchanges have transformed our perception of time and space. In the meantime, some new players have appeared in the arena, including the actual battlefields, which are more and more digitized and interconnected. In the same way, the decompartmentalization of the informational exchanges has led to the compression of the different levels of the operations design and control.

Considering the new threats raised regarding cyberspace and due to the increasing issue of informational supremacy, C2 structures must consequently be transformed in order to guarantee an ever more responsive decision-making and an ever more efficient execution of the military manoeuvers, despite new ethical and juridical considerations.

(PAGE VIERGE)

SOMMAIRE

(PAGE VIERGE)

Introduction

« *L'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre.* » Tel est le constat de Jean-Yves Le Drian, Ministre de la Défense, lors de son allocution à Bruz le 12 décembre 2016. En l'occurrence, notre manière d'aborder l'art de la guerre est consubstantielle à notre manière de la mener. Elle est donc intrinsèquement dépendante des outils mis à notre disposition pour le faire, en particulier des C2.

Préalablement à toute analyse, le concept anglo-saxon de C2 ou *Command and Control* doit être explicité. En effet, outre le fait qu'il puisse paraître tout à fait abscons au béotien, force est de constater qu'il en existe autant de définitions que de spécialistes autoproclamés du domaine. Tous conviendront néanmoins à dire que le C2 s'inscrit résolument dans l'action elle-même mais afin de mieux le cerner, il convient de s'attarder sur chacun des termes anglais *Command* et *Control.*

D'une part, *Command* se traduit sans difficulté par "commandement", c'est-à-dire la plénitude de l'autorité conférée à un Chef, de par son rang ou sa fonction, qui lui permet d'utiliser, en responsabilité, l'ensemble des ressources mises à sa disposition pour la réalisation de ses missions.

D'autre part, ce qui est simple par le truchement d'une traduction littérale de *Command*, l'est moins pour *Control*. En effet, la tentation première consisterait à le traduire par "contrôle", comme instillé dans le corpus doctrinal français[1]. Cela constitue une erreur, et dans l'esprit et dans la lettre, car le contrôle est soit « *l'action de contrôler quelque chose, quelqu'un, de vérifier leur état ou leur situation au regard d'une norme* »[2] donc se situe par définition si ce n'est en dehors au moins *a posteriori* de l'action elle-même ; soit « *l'action, le fait de contrôler quelque chose, un groupe, d'avoir le pouvoir de les diriger* » et se rapporte alors davantage au commandement. Aussi parler de « contrôle » n'a-t-il ici pas de sens en regard du concept de C2 et il conviendra en réalité de parler de « conduite » qui s'inscrit bien dans le déroulement de l'action elle-même : la conduite consiste en effet à orienter les forces et les systèmes au combat conformément à l'intention du Chef pour la réalisation de ses missions.

[1] DIA-01(A)1_DEF(2014), *doctrine d'emploi des forces*, §168, pp. 20 et suivantes et DIA-3(A)1_CEO(2014), *commandement des engagements opérationnels*, §4, pp.9 et suivantes ;
[2] Le Petit Larousse, Ed. 1998, page 258

Dans ces conditions, un système C2, désormais donc un système de *Commandement* et de *Conduite*, est un système intégré et global permettant au Chef de mener une opération. Il fut ainsi un temps où le C2 pouvait se résumer à des sonneries, des tambours, des drapeaux et des contingents de troupes consommables à merci. Le C2 moderne, quant à lui, bien plus élaboré et complexe, à bien des égards, et pour lequel l'économie des moyens est quasiment érigée en dogme, a été conceptualisé dans les forces armées américaines suite aux retours d'expériences de la Seconde Guerre mondiale et de la Guerre froide. Le C2 dont il est ici question, se rapporte en conséquence à l'ensemble des moyens humains, entraînés pour ce faire, associés à l'ensemble des systèmes d'information et de communication, de l'informations elle-même, du corpus réglementaire et doctrinal, des équipements et des installations dont un Chef a besoin pour conduire une opération. La globalité du périmètre du C2 est bien souvent déconsidérée et le C2est subséquemment circonscrit à un voire deux domaines. Pour éviter ces raccourcis, des compléments sont apparus : on a ainsi vu apparaître successivement le C3, puis le C4 et enfin le C4ISR. Or, à la lumière de la définition ci-dessus, on se rend bien compte que tous ces acronymes relèvent finalement du même concept de C2. Quant à l'usage du pluriel en parlant de C2, il illustre intrinsèquement la pluralité des opérations et, en corollaire, la pluralité des Chefs s'expliquant *a minima* par la diversité des milieux et la multiplicité des missions qui y sont réalisées.

Cela étant, à la révolution technologique de l'Internet ont succédé une révolution informationnelle et l'avènement du cyber. La fulgurance de ces phénomènes irrémédiables et incontrôlables met à mal le commandement et la conduite des opérations, d'autant plus que les technologies employées sont éminemment évolutives et constituent un vecteur permanent, instantané et universel de l'information, avec une portée indéniable de manipulations potentielles.

Car, désormais, « *les technologies de l'information et de communication rendent le contact, la collaboration et l'échange d'information si instantanés, si immédiats et si directs que les organisations pyramidales ne revêtent plus la même importance, ni le même rôle pour répartir les objectifs à atteindre et les objectifs à accomplir* » [3]. Tout n'est aujourd'hui que réseaux, la société elle-même se mue en « *société en réseaux* »[4], consolidée par « *la révolution informatique, la crise du capitalisme et de l'étatisme et l'essor de nouveaux*

[3] Bernard WICHT, *Europe Mad Mac demain ? Retour à la defense citoyenne*, Ed.Favre, Lausanne, 2013, p. 52 ;
[4] Manuel CASTELLS, *La société en réseau. L'ère de l'information*, Ed. Fayard, Paris, 1998, p.575 ;

mouvements sociaux et culturels»[5] toujours d'actualité. En ce sens, le monde change, a déjà changé et continue de le faire inexorablement. Il est indubitablement de plus en plus connecté, induisant nécessairement une accélération de la boucle décisionnelle, une imbrication des domaines d'action, « *un déclin des modes d'organisation pyramidale au profit de modèles plus plats, moins hiérarchiques* »[6]. De façon plus marquée et plus ténue qu'auparavant, toute opération militaire implique à la fois, directement et quasi instantanément, les acteurs militaires et non militaires, les autorités politiques, les médias, les organisations non gouvernementales, les sociétés civiles, et les opinions publiques.

Dès lors, le concept actuel de C2 des armées françaises est-il adapté à ces nouveaux défis ? La présente étude procède d'une réflexion personnelle visant à apporter une réponse à cette problématique, en d'autres termes à évaluer le concept de C2 dans le contexte actuel et à imaginer la mesure des changements qui devront lui être appliqués si nous voulons mener et gagner les guerres de demain. Il s'agit donc d'une confrontation praxéologique[7] entre l'expérience professionnelle de l'auteur, les analyses pratiques et les publications académiques et doctrinales portant sur le sujet, sans examen historiographique particulier. Aussi, de fait, l'essentiel de la réflexion s'inscrit-il à dessein dans le domaine militaire français contemporain.

Dans ces conditions, ce document s'articule autour de trois questionnements : l'avènement de l'ère de l'ère de l'information et le développement de l'environnement cyber conduisent-ils à une rupture et une mutation ontologiques (I) ? Dans quelle mesure les C2 contemporains en sont-ils affectés (II) ? Doivent-ils en conséquence être repensés afin de parfaitement intégrer les nouvelles conjonctures dans l'action (III) ?

*

* *

[5] Pierre MUSSO, Professeur d'Université à Rennes II et Paris I, compte-rendu dans la revue Quaderni, année 2000, volume 41, numéro 1, pp.147-150 ;
[6] Bernard WICHT, *Europe Mad Mac demain? Retour à la defense citoyenne*, Ed.Favre, Lausanne, 2013, p. 54 ;
[7] Au sens d'une théorie de la pratique, s'intéressant à l'agencement des moyens en fonction de fins précises et aux conséquences de l'action selon le contexte de son déroulement et des contraintes qu'il présente.

(PAGE VIERGE)

1. Entre rupture et mutations

La notion de rupture est intrinsèquement liée à celle de durée, conjuguée au principe d'incertitude. La rupture naît donc de la surprise. Intrinsèquement, elle conduit normalement à un bouleversement notoire, à un changement profond soit dans les processus soit dans l'organisation elle-même. En l'occurrence, la rupture stratégique est « *une mutation brusque et irréversible dans la représentation d'un antagonisme de niveau stratégique. Le changement doit être profond, d'où le terme de mutation. Celle-ci se déroule selon un processus rapide, ce qui légitime le terme de « rupture ». Elle s'impose comme irréversible, lorsqu'on ne peut plus faire comme si la situation n'avait jamais existé : on doit la comprendre et s'y adapter.* »[8]

Néanmoins, il faut se prémunir d'un changement de paradigme par trop violent, subit et subi. Aucun scénario n'étant totalement prédictible, les évolutions en cours doivent ainsi être constamment analysées et comprises. Cela ne suffit pas en soi et il importe également d'entretenir une certaine agilité de la pensée et des organisations pour rester en mesure de s'adapter rapidement à de nouvelles donnes.

Par ailleurs, une mutation est afférente à un changement radical, une conversion, une évolution profonde. Par définition, elle ne touche normalement qu'un volet de l'activité d'une organisation, avec des impacts plus ou moins importants. Combinées entre elles, plusieurs mutations concomitantes ou successives peuvent éventuellement conduire à une rupture.

Dès lors, les évolutions propres à l'avènement de l'ère de l'information, et du développement de l'hyper connexion de la société, dans tous les pans de l'activité humaine, relèvent-elles de la rupture ou de mutations ? Pour tenter de répondre à cette question liminaire, il faut procéder à l'analyse des changements opérés ou en cours de réalisation, selon différents aspects.

1.1. La lutte pour l'information

L'information est l'élément le plus caractéristique de la société en réseaux. Elle est partout, elle s'insinue partout, elle se partage instantanément. Elle structure en fait les relations humaines d'aujourd'hui. Les réseaux sociaux ont en effet eu l'avantage jusque-là inégalé de rapprocher les individus. Les liens familiaux et amicaux s'en sont ainsi renforcés et, souvent, des individus géographiquement ou socialement très éloignés, voire même qui ne se sont jamais rencontrés physiquement, sont en relations suivies sur la toile. Cet ensemble

[88] Olivier ENTRAYGUES (dir.), *La Rupture stratégique*, Études de l'IRSEM n°47, janvier 2017, p.34 ;

hétérogène constitue indifféremment les « amis » du réseau, qu'il convient d'avoir en plus grand nombre possible.

Ces « amis » transmettent, échangent et commentent toutes les informations qu'ils peuvent glaner sur les réseaux sociaux, dans une démarche tautologique effrénée. Ces informations sont mises à dispositions dans une banque de données non structurée, aux délimitations floues et libre d'accès, dénommée le « cloud », en référence à l'aspect informe et évolutif des nuages. Ces « amis » peuvent également être à l'origine d'une information diffusée sur les réseaux, soit parce qu'ils témoignent d'un fait qu'ils ont eux-mêmes observé, avec force photographies et vidéos à l'appui, soit parce qu'ils souhaitent partager une expérience ou une réflexion personnelle. Il y a en conséquence une multitude de citoyens-capteurs de l'information et la quantité d'informations disponibles sur le réseau des réseaux augmente de façon exponentielle. Pour illustrer cette multitude, Thierry Breton, le patron de la société d'Atos, estime qu'il y a aura d'ici peu autant de données numériques exploitables dans le monde que de grains de sable sur Terre[9]. Parallèlement, la communauté virtuelle est de fait devenue un acteur informel mais puissant de l'opinion publique et de la société.

Cependant que l'information est omniprésente, il est patent que la communauté virtuelle est de qualité très inégale en matière de traitement de cette même information qu'elle diffuse. En effet, cette information n'est que très rarement vérifiée et recoupée. Cela est vrai pour les « amis » les moins scrupuleux ou les moins rigoureux qui ne se contentent que de relayer les informations pour satisfaire leurs propres statistiques, pour augmenter leur influence au sein de la communauté ou, simplement, pour y exister. Mais cela est parfois vrai également au sein d'une communauté que l'on voudrait la plus méthodique sur le sujet, à savoir celle des journalistes. Ils doivent aussi exister et, pour ce faire, la compétition interne de celui qui sera à l'origine de telle ou telle annonce de quelque évènement s'opère parfois au détriment du professionnalisme. On se souvient ainsi de l'annonce de la fausse mort de M. Martin Bouygues par l'Agence France Presse le samedi 28 février 2015[10] : la réputation de l'agence n'étant alors plus à faire, l'information a été reprise par tous les médias, diffusée et commentée sur tous les réseaux sociaux, avant que l'AFP ne se confonde en excuses pour ce terrible malentendu tandis que M. Bouygues se portait à merveille. Cet incident mortifère

[9] Interview au Journal du Dimanche le 13 décembre 2015, sur http://www.lejdd.fr/Economie/Thierry-Breton-Prendre -en-main-le-destin-de-nos-donnees-763969, consulté le 16/12/2016 ;
[10] http://www.lemonde.fr/actualité-medias/article/2015/02/28/l-afp-et-la-mort-dementie-de-martin-bouygues-le-film-des-evenements_4585294_3236.html, consulté le 16/12/2016 ;

pour la notoriété de l'AFP illustre parfaitement le fait que l'information, quoiqu'omniprésente, n'en est pas pour autant d'une qualité et d'une véracité incontestables.

Quel qu'en soit le motif, la course à l'information peut donc conduire à la diffusion de faux bruits, dans des proportions gigantesques par le biais des communautés connectées et à une vitesse extraordinaire de par l'interconnexion des réseaux. Toutefois, ces faux bruits peuvent aussi être propagés intentionnellement. La puissance des réseaux d'aujourd'hui facilite en effet grandement la propagande délibérée, la manipulation des opinions publiques. La dernière campagne présidentielle américaine constitue un parfait exemple de l'utilisation volontaire, par les deux camps opposés du reste, des réseaux sociaux et médiatiques pour accabler l'adversaire de tous les maux, le plus souvent au travers d'informations biaisées voire fausses mais pas uniquement. Nous avons pu voir également étalées des informations des plus sérieuses mais volées grâce à ces attaques cyber toujours non revendiquées à ce jour : pour certaines, la pudeur et la décence auraient interdit leur publication ; pour d'autres, la fin politique justifiait les moyens peu recommandables usités.[11]

En définitive, tout individu, tout groupe, toute entreprise se retrouvent aujourd'hui submergés par une information pléthorique, d'une qualité discutable mais disponible à chaque instant. Aussi, l'enjeu est-il pour tous de parvenir à gérer ce flux incessant d'informations. Il s'agit en effet, non plus d'accéder à l'information comme ce fut longtemps le cas dans toutes les sociétés, mais bien de parvenir à séparer la lie de l'ivraie, à nourrir sa connaissance de renseignements de qualité. Pour y arriver, les défis sont nombreux car il s'agit à la fois de stocker toute l'information disponible, de l'analyser, de la discriminer pour enfin la purger de toute erreur. Le défi est immense, au regard de l'infinité relative de l'information, constamment renouvelée de surcroît. Dès lors, seule une intuition particulièrement affûtée, bien plus que la connaissance et l'analyse elles-mêmes, permettra de mieux embrasser le tout complexe, favorisant ainsi une approche globale plus efficace. L'intelligence humaine a certes des limites, mais l'intelligence artificielle que l'on met systématiquement en avant pour la gestion de l'information en a tout autant. Il est *in fine* inimaginable qu'un système d'information, aussi évolué et prédictif qu'il puisse être, parvienne un jour à égaler les capacités cognitives humaines permettant cette intuition requise en regard du flux incommensurable d'informations.

[11] http://www.lci.fr/international/cyber-attaque-entre-les-etats-unis-et-la-russie-obama-avait-pourtant-prevenu-poutine-2017784.html, consulté le 16/12/2016 ;

Dans un passé récent, il était aisé de maîtriser les informations et les médias car fondés sur des vecteurs lents et, compte tenu de la performance et des caractéristiques du réseau de réseaux actuel, l'information est finalement un véritable enjeu contemporain essentiel. On assiste à l'émergence d'un nouvel art de la« guerre » : la guerre de l'information qui « *consiste à dérober, détruire, pervertir l'information, depuis les connaissances intellectuelles jusqu'aux données informatiques. Son but est de produire un dommage, ou de gagner une hégémonie.* »[12]

1.2. Le développement du cyber

Support et moteur de l'économie mondiale, espace d'exercice des libertés fondamentales, nouvel enjeu militaire et de conflits, le cyberespace est un espace numérique qui constitue aujourd'hui un critère de puissance incontournable. Bien plus qu'un simple phénomène de mode, il est devenu l'espace à maîtriser. « *Dans ce nouvel espace, en expansion, en reconstruction permanente, composé de multiples couches, où, en apparence, chacun pourrait trouver sa place, les agrégats protéiformes, politiques, économiques et activistes s'affrontent d'ores et déjà selon un schéma qui tient tout à la fois de l'idéalisme, du constructivisme et du réalisme des relations internationales.* »[13] En l'occurrence, ce tournant stratégique a été matérialisé en France par l'apparition de la problématique cyber dans le Livre Blanc de la Défense et de la Sécurité Nationale de 2008, renforcée et clarifiée dans celui de 2013.

La notion de cyberspace regroupe plusieurs assertions qui peuvent être envisagées selon un angle technique et physique, cognitif et sémantique, stratégique ou encore juridique.

L'ANSSI[14] définit le cyberespace comme un « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées ». Dans cette définition orientée vers l'aspect technique, l'Internet physique n'est perçu que comme le support d'un espace de communication.

[12] François-Bernard HUYGHE, *Qu'est-ce que la guerre de l'information ?*, http://www.huyghe.fr/dyndoc_actu/4451ebfb7de54.pdf , consulté le 08/03/2017 ;
[13] Aymeric BONNEMAISON et Stéphane DOSSE, *Attention : cyber ! Vers le combat cyber-électronique*, Ed. Economica, Paris, 2014, p. 92 ;
[14] Agence Nationale de la Sécurité des Systèmes d'Information ;

Le Concept d'emploi des forces du CICDE[15] considère quant à lui que le cyberespace est « le réseau planétaire qui relie virtuellement les activités humaines grâce à l'interconnexion des ordinateurs et permet la circulation et l'échange rapides d'informations »[16].

Dans une démarche stratégique, le département de la défense américain qualifie le cyberespace de « *global common* », à l'image de l'espace, des eaux internationales et de l'espace aérien. Le cyberespace est donc considéré comme un espace accessible à tous mais détenu par personne, une ressource à laquelle tous les Etats ont un droit d'accès légal. Dans cette définition, le « *global common* » peut être de consistance géographique ou virtuelle.

Au-delà de ces définitions, ce qui caractérise le cyberespace, c'est la faculté qu'il offre d'opérer indifféremment au travers des quatre milieux physiques (mer, terre, air et espace), tout en s'affranchissant des frontières. Il peut être représenté selon un modèle en quatre couches :

- La couche physique qui regroupe les machines (terminaux, périphériques et objets connectés) et les infrastructures, serveurs et outils de connectivité (câbles sous-marins, réseaux sans-fil, datacenters, routeurs) ;
- La couche logique constituée des protocoles de communication, des systèmes d'exploitation et autres applications, des applications et services d'Internet (Web, Mail, partage de fichiers, messagerie instantanée) et des contenus et données ;
- La couche cognitive ou humaine formée de la perception, des usages et de la culture ;
- La couche C2, chapeautant l'ensemble des trois couches inférieures, et visant à coordonner l'ensemble aux fins d'obtenir un effet dans le cyberespace.

Le cyber est caractéristique des transformations liées aux technologies de l'information et de la communication sous les termes de société de l'intelligence, société de la connaissance ou société de l'information. « *Certains considèrent que cette mutation de l'outil de production est semblable à celle du néolithique (passage des sociétés de chasseurs-cueilleurs aux sociétés agraires) et à celle de la Renaissance (passage de l'âge agraire à l'ère industrielle). L'avènement de la société de l'information serait ainsi le troisième changement d'outil de production depuis 5000 ans.* »[17]

[15] Centre interarmées de concepts, de doctrine et d'expérimentations ;
[16] CICDE, *Concept d'emploi des forces*, CIA 01, 15 janvier 2010. ;
[17] Bernard Wicht, *Europe Mad Mac demain ? Retour à la defense citoyenne*, Ed.Favre, Lausanne, 2013, p. 50 ;

Par ailleurs, pour un cyber-pratiquant, voire un cyber-combattant, peu de moyens sont somme toute nécessaires. Les outils informatiques se sont en effet démocratisés tandis que les spécificités techniques des machines sur le marché ne cessent de se perfectionner à rythme soutenu, pour un coût toujours plus attractif. Un simple ordinateur personnel permet ainsi, grâce à la puissance du réseau de réseaux, d'interagir dans l'espace cyber. Pour autant, pour celui qui cherche à mener des opérations dans l'espace cyber, un niveau de technicité toujours plus accru est requis. En effet, au fur et à mesure que des failles de sécurité sont découvertes, elles sont systématiquement corrigées. On assiste donc à une course à celui qui exploitera telle ou telle faille d'une part avant les autres, d'autre part avant qu'elle ne soit rectifiée. La compétition est ainsi indubitablement rude dans la communauté des cyber-acteurs. Toutefois, ce que l'on nomme le « hacktivisme », en référence aux activités de hacking[18], est caractérisé par une très propension à partager les savoirs selon le principe du libre-échange. Dès lors, les différentes techniques éprouvées par la pratique de certains, sont ensuite mises à disposition de la communauté, tant et si bien que le niveau technique se perfectionne non seulement à l'échelle de l'ensemble du groupe mais aussi individuellement. Pour reprendre un exemple employé par M. Donald Trump durant la dernière campagne électorale américaine, il est à présent tout à fait possible pour un adolescent d'acquérir les compétences nécessaires pour mener, depuis sa chambre, des actions cyber aux proportions potentiellement importantes.

Car, puisque tous les systèmes, quel que soit leur domaine d'application, sont aujourd'hui fortement interconnectés, les « dommages collatéraux » d'une action cyber menée sur un élément du réseau sont mal maîtrisés. De plus, la non-imputabilité des actions est un des fondements incontournables de la manœuvre cyber : elle permet de mener des actions cyber en toute discrétion, permettant, sauf à les revendiquer pour des raisons diverses, de ne pas se dévoiler. Cela est d'autant plus problématique que les attaques cyber sont en général elles-mêmes d'une discrétion caractéristique, tant et si bien que le mal est bien souvent déjà fait lorsque l'alerte est donnée. Le ver informatique STUXNET[19] est un cas d'école en l'espèce puisqu'il semble que l'attaque ait été initiée en janvier 2009, qu'elle ait commencé à agir en

[18] Hacker est un terme emprunté à l'anglais et qui signifie « pirate informatique ». Un hacker est donc un fouineur, une personne qui a beaucoup de connaissances informatiques et qui peut pirater des logiciels informatiques, des sites web, etc. ;

[19] STUXNET a visé les centrifugeuses d'enrichissement de l'uranium de de la centrale nucléaire iranienne de Natanz. Après avoir recueilli toutes les informations utiles, il était programmé pour agir sur les commandes de conduite de fréquences des moteurs de ces centrifugeuses. Dans la durée, en changeant les vitesses, le code dégradait les centrifugeuses, leurrait les ingénieurs supervisant les opérations avec de fausses données et neutralisait enfin la production. Il aurait infecté entre 60000 et 100000ordinateurs, pour moitié en Iran. On ne sait toujours pas en attribuer la paternité, entre USA, Israël ou les deux conjointement. ;

juillet 2009, pour n'être finalement détectée qu'en juin 2010. L'originalité de cette attaque réside dans le fait qu'elle « *militarisait un procédé de cybercriminalité pour le transformer en mode d'action stratégique dans la profondeur d'un dispositif adverse.* »[20]

En définitive, le monde cyber s'est considérablement développé et il présente des risques nouveaux, d'envergure variable mais très souvent extrêmement dommageables lorsqu'ils sont exploités. Couvrir ces risques constitue subséquemment en enjeu prégnant pour la sécurité du réseau de réseaux, et, par voie de conséquence, pour celle de l'ensemble des systèmes qui régissent la société d'aujourd'hui.

1.3. La contraction du temps

Comme évoqué, l'intuition est un prérequis incontournable pour appréhender plus efficacement le « cloud » relationnel et informationnel. L'intuition est la connaissance directe et immédiate de la vérité s'affranchissant du raisonnement et de l'expérience. Elle est ainsi un pressentiment irraisonné et non vérifiable, fondé sur des brides d'informations mises en relation de façon inconsciente. Elle pousse à l'hypothèse de l'imminence d'un événement, voire de l'existence de quelque chose, et permet en conséquence une action visant à s'en prémunir ou à s'en servir. Pour s'affranchir du flux continu d'informations, qui plus est de qualité variable, l'intuition est donc primordiale pour l'action.

Toutefois, l'intuition ne naît elle-même que d'informations, fussent-elles parcellaires. Même si elle s'affranchit du raisonnement, elle a besoin d'indications pour se révéler. Ces indications ne peuvent pas, par essence, s'inscrire dans le temps long de l'Histoire puisqu'elles s'ancrent résolument dans le présent, pour mieux appréhender les potentialités de l'avenir. Il y a visiblement un paradoxe afférent au flux d'informations qui génère à la fois une inquiétude étourdissante de par son volume et son instantanéité, mais qui est tout à la fois requis pour l'action au travers de l'intuition. Le présent se densifie donc irrémédiablement.

En effet, bien plus que l'intuition, l'anticipation est devenue une pierre angulaire préalable à l'action. La recherche continuelle du renseignement se nourrit du flux d'informations disponibles. Compte tenu de la richesse et de l'accessibilité de la source, la priorité est donnée aux événements du présent pour ne pas nuire au rythme nécessaire de l'action. La rapidité des

[20] Aymeric BONNEMAISON et Stéphane DOSSE, *Attention : cyber ! Vers le combat cyber-électronique*, Ed. Economica, Paris, 2014, p. 59 ;

échanges, voire leur quasi-instantanéité, exige une capacité d'action et de réaction en corrélation avec ce nouveau rythme, là où l'intuition trouve de nouveau toute sa place.

Les différents rythmes qui décomposent l'espace pour former le Temps se confondent. Car le Temps est devenu un bien cyber en surabondance, disponible à loisir et consommable à l'infini. Densifié sur le présent, à une intensité directement proportionnelle à la vitesse luminique[21] des échanges et à celle des calculs désormais proche de l'exaflop[22], le Temps est portionné dans l'espace et se retrouve de plus en plus compressé. La notion de durée, désormais toute relative dans l'espace cyber, aurait ainsi seule encore une réalité pour l'intelligence humaine. Pour autant, cette durée doit être la plus courte possible dans la mesure où l'utilisateur, nourri de direct, de « temps réel », d'immédiateté, d'instantanéité, est de plus en plus impatient : tout doit lui être accessible en un clic. C'est qu'il n'a pas compris que l'opération de synchronisation qui nous fait parler au présent à l'échelle de planète, est au mieux une hypothèse, au pire une illusion, comme le conceptualisait Einstein dans sa critique de la simultanéité. Le temps s'écoule inexorablement, mais sa perception est biaisée : dans le monde cyber, il paraît comme compressé et recentré sur le présent.

Il existe cependant un paradoxe fondamental qui conduit à un écartèlement la notion de temps dans une dimension cyber : il est tout à la fois condensé, notamment grâce à l'instantanéité des échanges, et infiniment distendu, de par la mémorisation de toute donnée qui reste très longtemps, voire indéfiniment, disponible sur les réseaux.

1.4. La constriction de l'espace

Dès lors qu'il est connecté, le commun des mortels a la possibilité technique, grâce à la rapidité de transmission des signaux au travers des réseaux, de manipuler de façon instantanée plusieurs vues d'espaces réels. Il peut en effet juxtaposer une vue en temps réel de Shangaï, une d'Ankara et une autre de San Francisco, et passer de l'une à l'autre comme s'il y était. « *Il n'y a donc plus de hiérarchie, il n'y a plus de relation d'ordre entre les lieux réels,*

[21] En physique, relatif à la lumière ;

[22] Le FLOP est un acronyme anglo-saxon signifiant « opérations à virgule flottante par seconde », c'est-à-dire toutes les opérations qui impliquent des nombres réels. Depuis 2013, la machine la plus rapide du monde est chinoise, le Tianhe-2, qui atteint les 33,86 pétaflops (« péta» signifiant 10 à la puissance 15) : il réussit l'exploit de réaliser 33,86 millions de milliards d'opérations de calcul en une seule seconde. L'exaflop (10 à la puissance 19) qui fait l'objet d'une compétition rude entre les Etats-Unis, la Chine, le Japon et la France, pourrait vraisemblablement être atteint par l'un d'eux à l'horizon 2020. A titre de comparaison, un ordinateur personnel puissant atteint aujourd'hui plusieurs dizaines de gigaflops « seulement » ;

il n'y a plus de différence entre le près et le lointain »[23]. Tout étant ramené au point où l'on se situe, le temps s'y trouve également condensé puisque le déplacement en tant que tel n'est plus concevable.

Plus concrètement, « *le voyageur contemporain quitte un lieu sans suspendre nécessairement les interactions qui s'y déroulent. Il n'existe plus de coïncidence évidente entre l'éloignement en kilomètres et la rupture de l'effet de permanence qui le lie à ses proches.* »[24] Ainsi, où qu'il puisse physiquement se trouver, le voyageur d'aujourd'hui reste toujours centré sur son lieu usuel d'existence, tandis que ses « amis » quant à eux ont l'illusion de voyager par procuration au travers des informations, des photos et des vidéos échangées en continu. La perception de l'espace et l'évasion recherchée au travers du voyage se trouvent donc brouillées tant que le voyageur ne consent pas volontairement à se déconnecter des réseaux.

Toutefois, « *l'espace* [demeure] *une réalité tangible, malgré les moyens les plus modernes de mobilité* »[25]. Ce qui change, c'est la perception de cette réalité de par les notions de temps, d'éloignement physique, d'ubiquité, d'instantanéité, d'avatar, etc. De plus, même si sa nature virtuelle n'exclut pas une géographie physique propre au travers de sa couche physique, le cyberespace bouleverse également les délimitations de l'espace connu puisqu'il dépasse les frontières géographiques, sociales, politiques, étatiques. Le lieu d'une action n'importe plus autant qu'auparavant dans la mesure où elle peut désormais être ordonnée, suivie, voire réalisée à distance.

Par extension, un même espace, quelle que soit son envergure, peut être numérisé et concentré dans une visualisation infiniment plus petite. La localisation des actions qui y sont réalisées, et les actions elles-mêmes, peuvent alors être configurées à des milliers de kilomètres, comme si elles prenaient place tout juste derrière les écrans de restitution. Le mur d'images de la *War Room* du *Combined Air and space Operations Centre* (CAOC) de l'opération *Inherent Resolve* (OIR), reportant en continu le flux vidéo des dizaines de drones et autres capteurs en vol au-dessus du Moyen-Orient, donne ainsi l'illusion de frappes aériennes juste à l'extérieur du bâtiment alors qu'elles sont réalisées non seulement à l'échelle de tout le théâtre mais à une distance certaine de ce lieu de commandement et de conduite des opérations aériennes.

[23] Bertrand GUY, *A la recherche du cybertemps (réflexion sur le cyberespace)*, 2015. <hal-01175466> sur http://www.halshs.archives-ouvertes.fr , consulté le 06/02/2017 ;
[24] Fracis JAUREGUIBERRY et Jocelyn LACHANCE, *Le voyageur hypermoderne – partir dans un monde connecté*, Ed. érès, 2016, P.32 ;
[25] Kavé SALAMATIAN et Jérémy ROBINE, *Peut-on penser une cybergéographie ?*, Revue Hérodote, 2014/1-2 (n°152-153), pp 123-139 ;

Cela illustre bien le fait que, par le biais des moyens de communication modernes, l'étendue des théâtres n'obère plus la rapidité des échanges d'informations. De par la contraction du temps, ils frôlent au contraire l'instantanéité et permettent à leur tour une constriction grandissante de l'espace.

1.5. La métamorphose des systèmes hiérarchiques

Malgré des tentatives de décentralisation dans l'histoire récente, par exemple avec les lois Defferre de 1982, la France a depuis longtemps une tradition jacobine[26] et reste le pays le plus centralisé d'Europe. L'organisation territoriale complexe, conjuguée à l'apport considérable des technologies de l'information et des communications à l'ère de l'information, conduit inexorablement à une tendance davantage « girondine » par laquelle des pans entiers de responsabilités jadis du ressort de l'Etat centralisateur sont désormais reversés dans la sphère de compétence des territoires pour mieux répondre aux exigences de la société moderne et aux aspirations de la population. Néanmoins, s'il demeure un milieu dans lequel l'organisation centralisée et pyramidale demeure toujours incontournable, c'est bien le milieu militaire. Or, même ce milieu doit faire face à de nouveaux enjeux qui le conduisent à s'y adapter. Car, « *rigide quand on a besoin d'agilité, obtuse quand on valorise l'écoute, péremptoire quand l'échange est trop conservateur, la pyramide organisationnelle doit se transformer.* »[27]

En effet, le contexte budgétaire contraint, la professionnalisation de l'outil de Défense et la réduction induite des effectifs obligent à passer d'une logique de moyens à une logique de résultats. Il convient de s'intéresser davantage aux résultats concrets obtenus grâce aux moyens dédiés à une action plutôt qu'au volume de ces moyens. C'est la notion de performance qui prévaut donc, admirablement illustrée par la loi organique du 1er aout 2001 relative aux lois de finances (LOLF)[28] qui introduit une démarche de performance budgétaire. Ce phénomène est accentué par les apports technologiques propres à la diffusion de l'information dans la mesure où, les échanges étant facilités, l'obtention des résultats se trouve potentiellement accélérée, non plus au niveau de l'organisation elle-même mais au

[26] Le jacobinisme, opposé au girondisme, tient une bonne part de son origine durant la Révolution française. Les jacobins ont ainsi une vision selon laquelle l'Etat doit intervenir dans toutes les strates de la société pour influer sur la vie des citoyens et pour la réglementer, aux dépens d'une société civile en évolution libre. Certains penseurs, comme Edgar Quinet, estiment que le jacobinisme est un retour relatif à la monarchie absolue et à son organisation. Aujourd'hui, le jacobinisme décrit un Etat centralisé ;

[27] https://claudesuper.com/2014/09/17/organisation-la-faillite-du-systeme-pyramidal/, consulté le 28/01/2017;

[28] http://www.assemblee-nationale.fr/connaissance/ordonnace-finances.asp , consulté le 28/01/2017 ;

niveau de l'individu devenu élément central de production, quel que soit son positionnement hiérarchique. Bien évidemment, la coordination et l'arbitrage sont des notions indispensables dans un tel contexte, qui plus est dans une démarche militaire. L'organisation hiérarchique a donc toute sa place, même si son expression se trouve muée par rapport aux conceptions anciennes où seul le chef était à même de revendiquer quelque réalisation.

Ainsi, on assiste à une mutation de l'organisation pyramidale vers une organisation en réseau. Plusieurs intervenants, de qualifications et de statuts différents, sont connectés entre eux et accèdent instantanément à une information partagée, de telle sorte qu'ils sont mis en coopération pour la réalisation d'une mission précise, d'un ou plusieurs objectifs communs. Ces partenariats donnent naissance à une structure en forme de réseau coopératif et non hiérarchique, au sein de laquelle plusieurs parties autonomes se complètent et se mutualisent. La cohésion de l'ensemble naîtrait des interactions entre les différents acteurs et non plus de l'influence exercée par l'autorité. Cette organisation en réseau est d'autant plus nécessaire que la mission est complexe est difficile. La contraction du temps découlant de l'hyperconnexion de la société se traduit par le besoin d'une plus grande flexibilité. Cette dernière n'est désormais possible qu'en s'affranchissant d'une organisation par trop centralisée dont l'efficacité dépendrait en grande partie de sa porosité à l'information. Mais là encore, il faut néanmoins une structure centrale *a minima* qui distribue les rôles et définit les attributions et la nature des liaisons en contrôlant l'ensemble et supervisant la coordination entre les différentes parties.

De plus, la logique d'autorité a fait place à la logique de compétence métier. Là où l'autorité se suffisait à elle-même pour dicter les orientations prises par une organisation de type hiérarchique, s'impose dorénavant un besoin croissant d'expertises croisées. La fonction tend à primer sur le grade et donc sur la position hiérarchique. Qu'il s'agisse des transformations afférentes à l'avènement de l'ère de l'information, synonyme de mutations technologiques et organisationnelles, ou bien de l'affirmation des groupes armés issus des guerres irrégulières qui force l'outil militaire à tenir dûment compte de cette mutation d'envergure historique dans la définition de ses systèmes d'armes, toute décision repose sur l'avis d'experts de plus en plus spécialisés, de plus en plus répandus et de plus en plus autonomes en matière d'influence voire de décision. Cela mène donc soit à une sorte d'holacratie[29], s'apparentant à la mise en

[29] L'holacratie est un système d'organisation qui autorise la dissémination de la décision au travers d'une organisation fractale d'équipes qui s'organisent par elles-mêmes. La notion dérive de l'holarchie développée par Arthur KOESTLER dans *The Ghost in the Machine*, Ed. Penguin Group, 1967 ;

place d'organisations matricielles où de fortes connexions transverses sont en place alors que l'illusion de la pyramide classique est maintenue ; soit à un aplatissement de l'organisation pyramidale-type.

En définitive, « *les extraordinaires facilités de communication instaurées par la société de l'information conduisent à mettre le projet lui-même au centre des travaux : d'où la subordination des structures et de l'organisation à l'intelligence et aux idées. On passe ainsi d'une logique pyramidale de direction-gestion à une logique simplifiée de question-réponse.* »[30] Et « *ces premières considérations débouchent bel et bien sur un questionnement d'ordre ontologique : quelle est la forme d'organisation politico-militaire susceptible de suppléer aux anciennes structures, de garantir une prise de décision autonome et de redonner une base à la liberté d'action ?* »[31]

Selon la théorie de l'évolution selon Darwin, la sélection naturelle relève non pas de la loi du plus fort mais de la survie des mieux adaptés. Dans ces conditions, et par analogie, des structures organisationnelles plus hybrides, dans lesquelles une part beaucoup plus importante sera donnée à l'initiative personnelle, à la subsidiarité, apparaîtront nécessairement tout en demeurant une instance d'arbitrages et de décisions[32], afin de répondre aux nouvelles contingences découlant de l'avènement de l'ère de l'information car « *à la verticalité des hiérarchies succède l'horizontalité de la communication* »[33].

*

[30] Bernard WICHT, *Europe Mad Mac demain ? Retour à la defense citoyenne*, Lausanne, Ed.Favre, 2013, p. 52 ;
[31] *Id.*, p. 55 ;
[32] https://claudesuper.com/2014/09/17/organisation-la-faillite-du-systeme-pyramidal/, consulté le 10/02/2017;
[33] Manuel CASTELLS, *La société en réseau - L'ère de l'information*, Ed. Fayard, Paris, 1998, p.275 ;

2. La mise à l'épreuve des C2 « traditionnels »

2.1. Le C2 classique à l'œuvre

2.1.1. Le modèle de Barkhane

Le théâtre des opérations en Afrique comprend essentiellement Barkhane[34] mais œuvrent également dans la zone les forces de la TF SABRE, tandis que des forces sont également présentes au Sénégal, au Gabon, en République de Côte d'Ivoire et en République centrafricaine[35]. Pour chacune de ces opérations et pour chacun des territoires alentours, un commandant de forces (COMANFOR) est désigné. Trois particularités distinguent ce théâtre en regard de la doctrine en matière d'organisation du C2.

Tout d'abord, le niveau opératif et le niveau tactique de la composante terrestre sont fusionnés au sein du PCIAT de Barkhane à N'Djamena. Le niveau Brigade n'est en effet pas mis en place. Loin d'être problématique, ce mode d'organisation présente en réalité une efficacité remarquée en matière de commandement et de conduite puisque le fait de tout planifier de façon centralisée permet de coordonner la manœuvre interarmées jusqu'à la granularité la plus fine. En particulier, dans le domaine des SIC puisque le GTRS IA assure un commandement organique et fonctionnel de l'ensemble des détachements SIC déployés dans le cadre de l'opération, quelles que soient leur implantation et leur composante de tutelle. Recevant ses directives fonctionnelles du COMSICIAT, le GTRS IA est ainsi en mesure, grâce à un maillage particulièrement pertinent des systèmes de communications et des systèmes d'information, de coordonner l'intégralité de la mise en œuvre de la manœuvre SIC.

Ensuite, l'intégration de la troisième dimension réalisée par la composante aérienne est pilotée en réalité depuis la base aérienne de Lyon Mont Verdun au travers du JFAC AFCO. Le vieux concept « un chef, une mission, des moyens » ne tient plus avec la régionalisation et la centralisation du commandement des moyens aériens qui plus est lorsqu'il est à l'extérieur de la zone considérée. Dans ces conditions, un COMANFOR donné sur la zone d'opérations n'a l'OPCON des moyens aériens que durant les phases d'exécution des missions qui lui sont dédiées. En effet, un même aéronef peut désormais servir plusieurs COMANFOR au cours de la même mission, tout cela coordonner depuis la métropole. De plus, la possibilité offerte de mener des opérations à distance s'est concrétisée lors du premier tir opérationnel du lance-

[34] Le théâtre Barkhane couvre 5 pays (Mauritanie, Mali, Burkina Faso, Niger et Tchad), soit une superficie à peu près égale au double de celle de l'Europe continentale ;
[35] Un échelon de soutien national est maintenu à l'issue de la fermeture de l'opération SANGARIS le 01 novembre 2016 ;

roquettes unitaire (LRU) depuis Tessalit au Nord Mali, aux côtés d'un radar de l'escadron de détection et de contrôle mobile (EDCM). En effet, le commandement de tir a été donné à près de 2000 km, à N'Djaména (Tchad), tandis qu'un drone de l'escadron de Niamey (Niger) assurait le suivi de situation en temps réel de la zone de frappe. Ce tir visant des positions de groupes armés terroristes dans l'Adrar des Ifoghas (Est Mali) fut de surcroît un succès.[36]

Enfin, il faut se rappeler qu'il y a également des tensions fortes en Lybie voisine et des actions militaires peuvent y être menées sans néanmoins que ce territoire soit intégré dans une opération en tant que telle. Dans ce cas précis, le commandement de forces est alors assuré directement par le CPCO qui assure dès lors le C2 à la fois de niveau stratégique, de niveau opératif et de niveau tactique. Si cela est parfaitement réalisé à l'opportunité, il faut bien se rappeler que le CPCO n'est pas organisé ni dimensionné pour absorber ainsi les niveaux.

2.1.2. La gestion de crise sur le territoire national

La multiplication des acteurs qui sont à la fois capteurs, émetteurs et producteurs d'informations, la puissance des réseaux et la rapidité induite de transmission de l'information à tous les niveaux, impacte également la gestion de crise sur le territoire national.

Afin d'illustrer cet état de fait, il faut s'intéresser à un cas d'école d'une intervention autour d'un carambolage sur une route de montagne. En pareilles circonstances, l'information remonte très rapidement au centre de coordination des secours compétent qui prend évidemment toutes les mesures qui s'imposent. Dans le même temps, on l'imagine, ce carambolage a nécessairement créé un embouteillage conséquent. Les forces de gendarmerie sont en conséquence en ébullition non seulement pour sécuriser le lieu et éviter le sur-accident mais aussi pour établir des conditions de circulation alternative. Tous les centres opérationnels sont donc en alerte maximum pour gérer au mieux et au plus vite cette situation. Les forces sur le terrain sont également totalement engagées, forcément en situation de stress avéré. Or il se trouve qu'un homme politique de premier plan se trouve bloqué dans l'embouteillage et s'impatiente. Il passe donc quelques coups de téléphone et, finalement, c'est le préfet lui-même qui contacte directement les forces de l'ordre sur le terrain, faisant fi de toute hiérarchie opérative de coordination, ajoutant de fait une pression sur les opérations, au-delà de la pression médiatique déjà forte et des tensions compréhensibles existant sur le terrain.

[36] http://www.air-cosmos.com/barkhane-le-lru-a-l-oeuvre-65281, consulté le 26/11/2016 ;

Cette situation pourrait paraître anecdotique mais elle est en fait fondée sur nombre de cas concrets rapportés. Il n'est en effet pas rare de voir le niveau politique, donc le niveau stratégique, intervenir au niveau tactique, se substituant au niveau opératif. L'écrasement des niveaux est donc bien une réalité y compris sur le territoire national.

2.2. La compression des niveaux

Dans la conduite des opérations militaires, « la structuration du commandement en trois niveaux, répond à trois ordres de préoccupations distincts : le niveau stratégique placé à l'échelon politico-militaire, le niveau opératif, responsable de la cohérence et de l'efficacité de la campagne sur le théâtre, le niveau tactique qui conduit localement l'engagement des forces. »[37] En particulier, « le niveau opératif est l'émanation du niveau stratégique sur le théâtre d'opération. Ce niveau est garant de l'indispensable continuité entre les niveaux stratégique et tactique, ainsi que de l'interopérabilité avec les Alliés. Sur le théâtre d'opérations, ce commandement est le niveau d'intégration, de combinaison et d'évaluation des effets produits par l'action de la Force. Il vise à atteindre les objectifs fixés par le commandant stratégique et contribue ainsi à l'établissement d'une situation concrète souhaitée à la fin de l'opération (état final recherché). Le niveau opératif est donc le niveau d'intégration et de manœuvre de capacités militaires déterminées, afin de produire les effets voulus par le niveau stratégique dans une zone, une campagne et un environnement donnés. »[38] En clair, comme le disait Montgomery, « l'opératif rend tactiquement possible ce qui est stratégiquement désirable ». La doctrine édicte donc une structuration du commandement explicite mais il s'avère que les pratiques opérationnelles y dérogent de plus en plus, conduisant non pas à une dilution mais à une compression du niveau opératif, voire à un micro-management qui compromet la subsidiarité rendue nécessaire par les mutations de l'environnement des opérations.

2.2.1. L'implication grandissante du niveau stratégique

Puisque les informations remontent au plus haut niveau et de façon quasi instantanée, le niveau stratégique s'implique de plus en plus dans la conduite des opérations. Nous avons déjà évoqué le cas des opérations sur un territoire hors périmètre d'un théâtre défini et

[37] CICDE, *Doctrine d'emploi des forces*, DIA-01(A)1_DEF(2014), du 12 juin 2014, p.20 ;
[38] *Id.* p.21;

organisé, le cas de la Lybie en l'occurrence, pour lequel le CPCO endosse, temporairement l'intégralité des responsabilités de niveau stratégique, opératif et tactique.

Néanmoins, il ne s'agit pas là de cas isolés. En effet, de par la circulation extraordinairement rapide des informations, le politique, de façon générale, s'implique davantage dans les opérations. C'est en effet du fait du pouvoir de l'image et, subséquemment d'une reprise potentielle de la sphère médiatique, que le pouvoir politique affiche une tentation grandissante de s'immiscer dans la conduite des opérations militaires. Bien qu'il soit notoire que « *la guerre n'est qu'un prolongement de la politique par d'autres moyens* »[39], il ne faut pas se tromper dans l'analyse des conséquences d'une telle immixtion. Le temps des opérations est différent du temps politique qui, lui-même, se distingue du temps médiatique et judiciaire. Dans ces conditions, il y a une « *attente politique d'un résultat militaire rapide là où la résolution de crise nécessite souvent globalité et durée.* »[40]. Dès lors, le traitement militaire d'une cible particulière, la recherche d'un effet militaire particulier en vue notamment d'un effet médiatique donné, la modification du cadencement des opérations à des fins là aussi liées à l'image renvoyée auprès du public, sont autant de justifications pour le politique, et ce parfois jusqu'au plus haut niveau, d'interférer dans les opérations militaires. Cette situation est d'autant plus paradoxale que les armées doivent inévitablement mesurer leurs actions, tant vis-à-vis de la législation régissant les conflits armés qu'au regard de considérations éthiques et morales. L'immixtion trop pressante du politique dans les opérations conduit inexorablement à un surcroît de pression à laquelle les chefs militaires doivent faire face pour ne jamais malgré tout déroger aux règles du combat, pour se protéger, pour sécuriser l'action de leurs troupes et l'image qui en est renvoyée, et, *in fine*, pour protéger le politique lui-même de ses propres tentations.

Au-delà de cette analyse, Michel Foucault a renversé la thèse de Clausewitz lorsqu'il annonça que « *c'est la politique qui est la continuation de la guerre par d'autres moyens, et non l'inverse.* » La résolution de crise s'inscrit en effet dans le temps long, et l'histoire nous a montré que l'action militaire par elle seule n'en a résolu aucune. Pour autant, l'accélération du tempo des opérations, qu'elles soient militaires ou politico-médiatiques, en particulier du fait de l'avènement de l'ère de l'information, conduit à une juxtaposition voire une fusion des thèses en réalité complémentaires de ces deux penseurs. Il est subséquemment

[39] Carl Von CLAUSEWITZ, *De la guerre*, Ed. Librairie académique Perrin, 1999, p.37 ;
[40] Audition du général Jean-François PALANTI, directeur du centre interarmées de doctrines et d'expérimentations, auprès de la Commission de la défense nationale et des forces armées le 03 décembre 2014 ;

particulièrement important de maintenir un niveau élevé de vigilance pour que les actions d'un acteur ne nuise pas à l'autre, et réciproquement. La maîtrise du tempo opérationnel est consubstantielle de la maîtrise informationnelle, ce qui nécessite agilité intellectuelle et anticipation de toutes les parties.

2.2.2. Les écarts du niveau tactique

Par ailleurs, la tentation est parfois grande pour le niveau tactique d'entretenir une relation directe avec le niveau politique à dessein. En effet, résolument engagé dans une action régie par le tempo informationnel, l'échelon de commandement au plus près du terrain peut se retrouver en situation d'obtenir des orientations voire un aval direct de l'échelon décisionnel le plus haut, et s'affranchir ainsi des échelons intermédiaires jugés parfois ralentis par les procédures, les processus de planification, et les lourdeurs administratives induites par le fonctionnement d'états-majors intermédiaires estimés peu réactifs. Il s'agit là de comportements conjoncturels et peu fréquents en réalité, mais cela n'enlève en rien les problématiques qu'ils infèrent à différents niveaux de considération.

Au-delà de ces comportements, il est, encore plus aujourd'hui qu'auparavant, des situations où, nécessairement, le niveau tactico-opératif est en relation directe et ténue avec le niveau stratégique dans la conduite des opérations.

Cela est par exemple particulièrement avéré dans le cadre des opérations spéciales qui, par nature, exigent de telles connexions. Pour autant, l'interconnexion des réseaux et le flux d'informations à partager, alliés à la recherche d'effets utilisant des moyens de plus en plus conjoints, nécessitent une coordination de niveau opératif accrue afin de combiner au mieux les actions et d'intégrer les effets des différentes composantes.

De même, le contrôle national des actions menées par les forces françaises au sein d'une coalition nécessite, en conduite, une liaison ténue avec le niveau politico-stratégique. En effet, dans le cadre de l'opération *Inherent Resolve* au Levant, le directeur du CAOC d'Al Udeid exerce le commandement tactique (TACOM) et le contrôle tactique (TACON)[41] sur l'ensemble des aéronefs de la coalition. Il est donc essentiel pour le responsable de la conduite des opérations aériennes nationales au sein du CAOC d'être en contact avec le niveau stratégique pour la validation, en temps réel, d'objectifs dont la décision ne lui est pas déléguée, en particulier au cours de missions dynamiques de Close Air Support (CAS).

[41] CICDE, DIA-01(A)_DEF(2014), Doctrine d'emploi des forces, 2014, p.34 §414-415 ;

Ainsi, les interactions entre niveaux de conduite et niveaux décisionnels hauts, dans les sens montants come descendants, sont une réalité et une nécessité. Cela est d'autant plus avéré que les technologies de transmission de l'information permettent des échanges quasi instantanés, qui plus est sur la base d'informations qui sont plus en plus délicates à cloisonner.

2.2.3. L'essentielle subsidiarité

Dans l'antiquité, le « subsidium » était une méthode d'organisation militaire selon laquelle une ligne de troupe se tenait en alerte à l'arrière du front, prête à porter secours en cas de défaillance. Plus tard, Aristote décrivit, dans *Les Politiques*, une société organique au sein de laquelle des groupes aspirant à l'autosuffisance s'emboîtent hiérarchiquement. Par-là, il définit la notion de subsidiarité telle qu'elle est dorénavant déclinée au sein des organisations politiques, économiques, sociales et militaires. Il s'agit aujourd'hui de donner le pouvoir et la responsabilité de décision et d'action à l'entité qui est la plus proche de l'opérateur, de la personne ou du groupe considéré. Partant, la subsidiarité est distincte de la délégation puisqu'au travers de cette dernière, l'échelon supérieur offre à l'échelon inférieur le loisir de l'exécution d'une tâche tout en en conservant l'entière responsabilité. En réalité, comme la définit l'institut Montalembert[42], la subsidiarité répond à trois principes :

- Principe de compétence : l'échelon supérieur s'interdit toute tâche que peut accomplir par lui-même l'échelon inférieur ;
- Principe de secours : l'échelon supérieur doit soutenir, si nécessaire, et peut aider l'échelon inférieur ;
- Principe de suppléance : exceptionnellement et de manière limitée dans le temps, l'échelon supérieur peur remplacer l'échelon inférieur en cas de défaillance.

Au regard de l'ubiquité d'une information pléthorique, d'une réduction continue des effectifs militaires, de la complexité des conflits asymétriques, et du tempo accéléré des opérations, un chef ne peut plus concentrer à son seul niveau toutes les décisions, sous peine de saturation par surinformation. En réalité, les responsables, quel que soit leur niveau hiérarchique, doivent désormais coopérer de façon de plus en plus ténue. « *L'autorité supérieure doit s'exprimer en promouvant la marge d'initiative et de responsabilité de l'échelon subalterne : cela implique de donner du sens aux ordres pour en permettre une réception intelligente et réactive.* »[43]Car c'est l'acteur au plus près de l'action qui est le plus à même de savoir ce qu'il

[42] http://www.institut-montalembert.fr/economie/subsidiarite-et-management-286/, consulté le 22/02/2017;
[43] Cf. doctrine sociale de l'Eglise et engagement militaire – http://www.dioceseauxarmées.fr, consulté le 22/02/2017;

peut concrètement faire pour réaliser la mission, dans des délais compatibles avec la nouvelle donne de l'ère de l'information. En effet, l'autonomie en matière de décision revêt une importance d'autant plus grande que le contexte d'engagement des forces place les Armées sur le terrain au cœur des populations et exige des prises de décision rapides[44], y compris dans une cadre interarmées, interalliés voire interministériel.

Par la puissance du réseau qui est par définition connecté, l'information vient de n'importe où, pour aller n'importe où, par n'importe quel chemin : il y a donc une infinité de voies subsidiaires pour distribuer l'information, qui plus est de façon quasi instantanée. Le principe de subsidiarité s'en trouve d'autant plus prégnant dans la mesure où chaque échelon dispose potentiellement au même moment des mêmes informations permettant l'appréciation de situation. La vicariance des voies de communication, c'est-à-dire leur capacité à trouver des voies subsidiaires lorsqu'un obstacle s'interpose à la circulation de l'information, accentue encore plus ce phénomène. Le partage des informations ainsi disponibles permet d'obtenir une compréhension opérationnelle commune, partagée par les différents échelons hiérarchiques, qui facilite potentiellement la décentralisation des décisions. Tous les échelons sont donc mis à contribution, chacun avec un cycle décisionnel raccourci et optimisé du fait de l'utilisation de systèmes performants de recueil et de transmission de l'information.[45] Ils agissent en parallèle, focalisés sur les tâches de leur niveau, toutes ces tâches concourant à la réalisation du même objectif. Dans ces conditions, le tempo des opérations est mieux maîtrisé et l'économie de moyens est caractérisée.

Face à un adversaire qui dispose quasiment des mêmes avantages informationnels, la plus grande réactivité, l'adaptation et la capacité de réponse sont primordiales pour gagner et conserver quelque avantage. Dès lors, seule une subsidiarité affirmée et assumée, combinée évidemment à des mesures organisationnelles et doctrinales, permet cette agilité. La planification et la conduite opératives s'en trouveraient donc compromises car, dans le cas d'une telle subsidiarité, le niveau tactique de composante pourrait être à même de traduire directement les objectifs stratégiques en effets. Dans ce cas, la coordination des actions des composantes sur le terrain est primordiale et elle pourrait être assurée par le niveau stratégique, à l'instar du cas libyen évoqué supra.

[44] Tiphaine GRALL, *La numérisation dans les Armées : similitudes et disparités des doctrines nationales*, Doctrine n°14, janvier 2007, pp. 107-111 ;
[45] Pierre GOETZ et Olivia CAHUZAC-SOAVE, *Impact de la numérisation sur l'exercice du commandement*, Les notes stratégiques, CEIS, janvier 2016, page 16 ;

De cette nécessaire subsidiarité et de l'apport technologique est apparue la notion de « caporal stratégique » mais il s'agit là d'une illusion de la transformation digitale des armées. La subsidiarité sous-tend l'initiative de la part d'intégrateurs rendus de plus en plus nécessaires dans un monde en perpétuelle incertitude. Aussi, ce n'est pas d'un « caporal stratégique » qu'il s'agirait, mais, a minima, d'un « capitaine stratégique » afin de répondre parfaitement et justement aux exigences du moment.

2.3. L'action confrontée au réel

2.3.1. Le choc de l'information

La place de l'information dans les opérations militaires n'est pas une nouveauté puisqu'elle a toujours représenté en réalité une priorité, notamment en regard de l'avènement de nouveaux systèmes d'arme. Les militaires ont toujours recherché la meilleure performance en matière d'observation et de communications. A titre d'exemple, il faut se rappeler la mise en place en 1854 du télégraphe électronique durant la guerre de Crimée, voulue par Napoléon III, et placée sous la férule du Ministère de la Guerre tant les potentialités d'ordre militaire étaient déjà perçues.

Aujourd'hui, la supériorité informationnelle est un enjeu majeur dans les opérations. Les capacités de traitement et d'échange de l'information sont en ce sens primordiales, une impérieuse obligation aux fins d'acquisition d'une position de supériorité vis-à-vis d'un adversaire qui, de son côté, aurait les mêmes objectifs. La principale difficulté réside non seulement dans le volume incroyablement conséquent des informations disponibles, notamment du fait de la multiplication des capteurs, mais aussi dans le flux et la vitesse de transmission desdites informations grâce à la performance des réseaux. Les Américains se sont essayés à maîtriser cette information pléthorique mais ont été contraints de se résoudre à d'autres approches. En effet, en mettant en place le renseignement électronique dans les années 1990, ils avaient estimé que le renseignement utile serait plus facilement accessible s'ils écoutaient l'ensemble des informations circulant dans tous les réseaux. Cette position n'étaient pas nouvelle dans la doctrine américaine puisqu'une première base du système d'écoute Echelon vit le jour dans les 1970, dans un contexte de Guerre Froide et dans la droite ligne accords UKUSA[46] de 1947. Pour autant, même si ces actions d'espionnage ont

[46] *United Kingdom-United States Communications Intelligence Agreement* : les négociations entre britanniques et américains concernant un accord SIGINT (signal intelligence) en temps de paix, débutèrent dans l'immédiat

indubitablement permis de mettre au jour des renseignements utiles, elles demeurent aujourd'hui bien maigres en regard de l'immensité de l'océan informationnel, d'autant plus que le système de traitement et de sélection est fondé, entre autres, sur la détection de certains mots clés. En simplifiant le raisonnement, sans aucun mot clé, le système aurait plus de peine à distinguer l'information utile du tout-venant.

Parallèlement à ces difficultés, c'est le besoin sans cesse croissant d'information, à tous les niveaux, qui est aussi problématique. En effet, un renseignement de niveau stratégique peut revêtir un caractère immédiatement opératoire au niveau tactique, et *vice versa*. La ségrégation de l'information demeure donc un défi notoire, mais la maîtrise des flux également. Plus généralement, dans la société en réseaux de réseaux, l'information est devenue un objet de consommation courante, qu'on échange, qu'on transfère et qu'on jette sans scrupules puisque d'autres informations arrivent en flux continu. On absorbe de l'information sans faim, on ne capitalise que très peu. Dans les opérations militaires, il est donc indispensable de veiller à ce que l'information utile soit le plus valorisée possible de façon à la distinguer du flux courant et, ainsi, d'en garantir l'exploitation à temps par un échelon donné.

2.3.2. La judiciarisation de l'action

L'information judiciaire ouverte en 2012 à propos de l'embuscade d'Uzbeen en Afghanistan a mis au jour un décalage croissant entre les contingences de l'état de militaire, en particulier en opérations, et le droit commun. Il ne s'agit pas ici de débattre de l'opportunité d'occurrence d'une telle manifestation, mais pour mieux en cerner les contours, il faut tout d'abord préciser le périmètre de cette question.

La pénalisation de l'action militaire serait un phénomène « corrélatif à la sacralisation de la victime et au rejet de l'aléa, abusivement confondu avec le trop fameux principe de précaution » tandis que la judiciarisation serait « *l'instrument par lequel la société civile tend à imposer sa sacralité à la communauté militaire et à la contraindre en conséquence à renier certaines de ses valeurs fondamentales.* »[47] En d'autres mots, et par voie de conséquence, l'excuse pénale des militaires engagés dans une mission de combat et faisant usage de la force

après-guerre en septembre 1945. D'autres pays les rejoignirent par la suite, dont la Norvège, le Danemark et l'Allemagne concernant l'Europe.

[47] Christophe BARTHELEMY, *La judiciarisation des opérations militaires*, Thémis et Athéna, Ed. L'Harmattan, 2013, p.158 ;

pourrait être remise en question, et ce malgré une application stricte des règles du droit internationale en la matière.

En première approche, il est aisé d'en conclure que la décision d'un chef sur le terrain, décision menant à l'action physique, pourrait être suspendue à l'analyse des conséquences éventuellement judiciaires qui en découleraient. Cela aurait pour conséquence de faire surgir un risque d'inaction ou d'action décalée, là où agilité et célérité demeurent incontournables pour la réalisation d'effets donnés. Bien évidemment, ces considérations de légitimité et de légalité de l'action conditionnent déjà normalement l'action du chef militaire puisqu'elle doit se conformer au droit des conflits armés, incluant le droit humanitaire et le droit de la guerre. Toutefois, la problématique survient lorsque ces considérations dépassent le seul cadre légal régissant l'action au combat et versent dans une crainte de poursuites dans un champ différent. Cela est d'autant plus préoccupant que le champ des possibles, l'étendue des incertitudes s'accroissent, en d'autres termes, que le brouillard de la guerre s'épaissit, à mesure que le flux d'informations augmente. Le risque est donc réel, si l'on n'y prend garde, de perdre la décision du chef en conjectures autour d'une quantité d'informations et de possibilités qu'il ne serait plus en mesure d'analyser de façon exhaustive. Il est donc essentiel de « *restaurer un équilibre stable entre principe de légalité et réalisme des principes*»[48] pour protéger l'action militaire au combat au travers du seul périmètre législatif *ad hoc*. En parallèle, il convient de mettre sur pied l'ensemble des leviers nécessaires à la limitation des risques « *d'instrumentalisation de l'action judiciaire par des acteurs qui auraient intérêt à contester par ce biais la politique militaire française.* »[49]

Par ailleurs, cet atermoiement est d'autant plus prégnant dans la construction des modes d'actions du chef que l'information née de son action est, potentiellement, immédiatement et universellement transmissible et donc exploitable. En l'occurrence, l'adversaire doit être réputé tout aussi habile à capter l'information, l'analyser voire la travestir à des fins opératives. La manipulation de l'information, procédant ou pas d'actions de propagande, est une réalité avec laquelle il faut composer.

2.3.3. L'étreinte éthique

Au-delà des seules considérations juridiques, et des éventuels actes répréhensibles relevant du droit commun, il circule l'idée d'une accentuation de la brutalité de l'action militaire, d'un

[48] *Id.* page 153 ;
[49] Projet de loi de programmation militaire 2012 ;

relâchement des considérations éthiques lors d'interventions dans des conflits dits asymétriques ou urbains. Est-ce seulement du fait d'une altération de l'*ethos* militaire ou bien d'une modification de la perception des sociétés à l'égard de l'usage de la force ?

Quoi qu'il en soit, la pression sociétale axée sur le respect de la vie humaine a entraîné une accentuation du contrôle interne dans les armées. En outre, ledit contrôle interne s'est également renforcé du fait du retour d'expériences des épisodes bosniaques ou rwandais, durant lesquels les forces françaises ont été directement mises en cause qui pour passivité qui pour complicité d'acte de génocide. De plus, de la fin de la conscription et du passage induit à une armée de métier, est née une exigence de professionnalisme et du respect des valeurs morales, consubstantielle à un contrôle renforcé.

Il ne s'agit pas, néanmoins, pour les échelons de commandement des armées de s'interdire l'action sous couvert de contrôle interne, mais bien d'une parfaite intégration des normes éthiques que la société exige, d'une ambition affichée de s'assurer de l'instillation de cette intégration jusqu'à l'échelon d'exécution le plus bas.

Il n'en demeure pas moins qu'il existe un rejet foncier de la société pour la perte de vies humaines parmi les populations civiles. Même si les processus de ciblage sont aujourd'hui rôdés et bien appliqués, même si les processus[50] et les évolutions technologiques permettent l'utilisation d'armes de précision limitant les dommages collatéraux, il existe en permanence un besoin du politique de tenir dûment compte de l'opinion publique. En l'occurrence, nombre d'images parvenant des zones de conflictualité où nos troupes sont engagées sont diffusées par les médias. Sous couvert du droit à l'information et de la liberté des médias, se cachent souvent des réalités économiques justifiant une course à l'information incompatible, en l'espèce avec un discours mesuré en commentaires de ces images, voire ne serait-ce qu'une vérification des sources. Il en résulte un risque de plus en plus présent de manipulation de l'opinion publique, parfois indirecte et pas forcément délibérée, qui peut conduire à une mise à l'index de l'action des troupes engagées. Ce phénomène est naturellement accéléré grâce aux potentialités offertes aujourd'hui par les réseaux de communication et par la démultiplication des capteurs.

Dès lors, du chef militaire en opérations au soldat au combat, tous se retrouvent pris dans un étau éthique avec, d'une part, un contrôle interne accru, et, d'autre part, une pression

[50] CICDE, PIA-3.9.9_EDC(2014), *Estimation des dommages collatéraux*, 2 juillet 2014 ;

médiatique avide du moindre incident susceptible d'animer quelque débat et pouvant conduire à un resserrement de l'étreinte en cas d'emballement des opinions.

2.3.4. Les failles des systèmes d'armes

L'utilisation des réseaux, qui plus est de plus en plus interconnectés, participe d'une formidable amélioration des capacités d'action des armées modernes. En effet, la circulation de l'information y est de fait considérablement facilitée augmentant ainsi l'aptitude à conduire les opérations sur la base d'une situation de théâtre mise à jour de façon quasi-instantanée. Toutefois, tandis que l'interconnexion des réseaux augmente leur résilience de par les redondances ainsi construites, elle pose paradoxalement deux difficultés majeures.

La première réside dans le nécessaire décloisonnement pour un partage de l'information pertinent. Ce décloisonnement se décline lui-même d'abord au niveau national puisque la tentation fut grande pour chaque composante de travailler l'information brute à son niveau pour en tirer des avantages opératifs propres. Ce postulat ne tient plus dès lors que les opérations d'aujourd'hui ne peuvent s'entendre uniquement selon une couleur unique d'armée. De plus, ce décloisonnement est rendu nécessaire par l'impérieuse obligation d'interopérabilité entre les systèmes de combats, tant interarmées qu'interalliés. De cette interconnexion naît alors de nouvelles fragilités sur nos propres systèmes puisque leur sécurité et la sécurité induite des informations en partage, reposent désormais en grande partie sur les mesures prises par nos partenaires.

La seconde repose sur l'augmentation de la surface de vulnérabilités et de la surface d'attaques[51] de par l'émergence de nouvelles menaces fondées sur la multiplication des portes d'entrée au travers de l'interconnexion des réseaux. Cet accroissement des vulnérabilités est d'autant plus problématique pour les Etats que les adversaires auxquels ils doivent désormais faire face, clairement non-étatiques ou Etats faillis, ont indéniablement beaucoup moins de systèmes à protéger. Il y a là donc une dissymétrie des vulnérabilités en défaveur des systèmes de forces étatiques qui enjoint les Etats à consacrer toujours plus de moyens et d'énergie à la sécurisation de leurs réseaux.

Concomitamment à ces risques nouveaux induits par l'usage des réseaux, force est de constater que les systèmes d'armes modernes utilisent de plus en plus des logiciels et autres progiciels numériques. Or, dès lors qu'un processus est construit autour de codes

[51] https://www.information-security.fr/analyt-reduction-surface-dattaque/ , consulté le 01/03/2017 ;

informatiques, il devient de fait une cible potentielle et il est ainsi davantage vulnérable aux attaques. La numérisation des outils de combat, si elle a permis une amélioration indéniable de leurs capacités, de leur employabilité et de leur efficacité, ne les en a pas moins « fragilisés » et ouverts à de nouvelles menaces. Il faut se souvenir du piratage probable (non revendiqué) en 2015de batteries de missiles *Patriot* allemandes déployées en Turquie, pour pleinement mesurer l'ampleur du risque encouru.

Par ailleurs, outre les systèmes purement militaires, c'est l'ensemble des domaines sociaux et économiques qui s'aventure dans la révolution numérique et dans l'usage du réseau des réseaux informationnels. Ces domaines sont subséquemment davantage exposés aux risques de piratages, voire de cyberattaques, dont les conséquences, peu mesurables aujourd'hui, impacteraient inéluctablement les organes de défense, par effet de cascade. La protection des systèmes d'information est donc devenue un enjeu de sécurité nationale. En France, la création de l'ANSSI[52] en 2009, rattachée au SGDSN[53] donc au Premier ministre, illustre la pleine ampleur de l'enjeu dans la mesure où elle a compétence non seulement sur les structures étatiques, au premier rang desquels la Défense, mais aussi sur les opérateurs d'importance vitale (OIV) parmi lesquels figurent les grands groupes industriels nationaux.

* *

[52] Agence nationale de la sécurité des systèmes d'information
[53] Secrétariat général à la défense et à la sécurité nationale

(PAGE VIERGE)

3. Les enjeux des C2

L'ère de l'information et l'avènement du cyber ont-ils des conséquences sur les espaces d'affrontement non seulement contemporains mais surtout à venir ? Les territoires nationaux ne sont plus des sanctuaires et ils peuvent être attaqués directement, y compris anonymement, par des puissances étrangères, des organisations criminelles, des groupes ethniques, des associations de malfaiteurs. Cela est d'autant plus préoccupant que la numérisation, la digitalisation des armées va bon train, en même temps que le flots d'informations s'accroissent continuellement. Même engagées dans des conflits traditionnels, les armes cinétiques ne constituent qu'une partie seulement de l'arsenal disponible à opposer à l'adversaire. L'espionnage électronique, le sabotage, les opérations de manipulations rendues possibles par les médias de masse, la diversion numérique, et l'attaque des systèmes C2 adverses par des hackers spécialement diligentés, constituent autant de moyens pour neutraliser une grande partie des forces adverses, tout en permettant de concentrer l'usage des moyens cinétiques aux seuls instants et lieux qui le nécessitent pour obtenir l'effet final recherché.[54]

Toutefois, ce que nous sommes ou serons en mesure d'opposer à nos adversaires dans cet environnement numérisé et connecté, nous est en retour parfaitement opposable et nos C2 de demain devront en conséquence répondre à des exigences cruciales.

3.1. La nécessaire agilité des C2

Les C2 doivent être éminemment agiles, étant entendu que l'agilité procède de la combinaison entre robustesse, résilience[55], flexibilité, innovation, adaptation et capacité de réponse.

L'apparition de « *la guerre hybride, caractérisée par la mise en œuvre de moyens de destruction, d'intrusion et d'espionnage du cyberespace en vue d'affaiblir ce qu'on attaque* »[56] a bouleversé le champ des possibles en termes de manœuvres opératives, et, en conséquence, a rendu les mesures de sécurité encore plus fondamentales pour les C2 modernes. Dans le même temps, plus que la gestion, la maîtrise de l'information est devenue essentielle à tous les stades de quelque manœuvre que ce soit.

[54] David S. ALBERTS, *The unintended consequences of information age technologies*, Ed. University press of the Pacific, 2004, pp 15-28 ;
[55] Tout en constituant en mécanique la résistance d'un matériau au choc, ou encore en zoologie la faculté d'une espèce à se reproduire malgré un environnement hostile, la résilience est plus généralement la capacité pour un individu ou pour un système à faire face à une situation difficile, à rebondir face à l'adversité. Elle entraîne la défense-protection, l'équilibre face aux tensions, l'évaluation, la relance, la création ;
[56] http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415026.asp, consulté le 18/01/2017;

3.1.1. Un cyberespace hostile

Le cyber constitue à la fois un espace extraordinaire de potentialités, y compris d'ordre militaire, et une source de menaces diverses. Car, dans cet espace, des opérations particulières peuvent être et sont d'ores et déjà menées. Les romans à succès de science-fiction, de Marc Elsberg[57] à Tom Clancy[58] pour ne citer qu'eux, n'ont plus l'apanage de ces scénarios opératifs décrits dans l'espace cyber, devenu par la force des choses, une réalité.

En l'occurrence, on peut y distinguer d'une part la cyberguerre, une guerre d'ordre strictement militaire suivant les principes relatifs à l'information. Il s'agit ainsi de « *conduire des opérations militaires suivant des principes relatif à l'information. C'est-à-dire détourner ou détruire l'information et les systèmes de communication adverse.* »[59] En ce sens, l'exploitation des failles de sécurité des systèmes d'information vise, entre autres, cette altération de l'information. Cela constitue un des piliers de la compétition technologique mondiale car il s'agit à la fois de développer des « cyberarmes », entre logiciels espions, logiciels malveillants et systèmes d'écoute, tous suffisamment discrets pour pouvoir agir le plus longtemps possible et en toute discrétion, tout en se protégeant de ces mêmes « cyberarmes » lancées par les adversaires potentiels. La principale difficulté dans la cyberguerre, c'est précisément qu'elle doit demeurer silencieuse et pernicieuse. Qui aurait pu imaginer que de telles opérations puissent être menées par la Russie à l'encontre des Etats-Unis, dont certaines ont pu être révélées à demi-mots durant la dernière élection américaine ? La suspicion est donc globale et la course à laquelle on assiste à travers le monde en la matière est inquiétante. La Chine compterait déjà une cyberarmée de plus de 20000 hommes, renforcée d'un réseau très actif d'universités, de centres de recherche et de services de renseignement. Le Cyber Command américain planifie de multiplier ses effectifs par cinq. Tandis que la Ministère de la Défense, à lui seul, a dénombré plus de 24000 attaques informatiques externes en 2016, le gouvernement français a décidé en décembre 2016 de créer le Cybercom, commandement fonctionnel mais dont les ambitions sont visiblement organiques puisque l'idée d'une quatrième armée est officiellement abordée.[60] Au-delà de ces quelques exemples, on assiste à un emballement planétaire autour de la question, une compétition sourde mais bien réelle dont l'issue est incertaine si ce n'est l'inexorable développement technologique que cela sous-tend. Certains osent même parler d'une gestation de cyberguerre froide mondiale.

[57] *Eg*. Marc ELSBERG, *Black Out – Demain il sera trop tard*, Ed. Piranha, 2016 (2e édition)
[58] *Eg.* Tom CLANCY, *Cybermenace*, Ed. Albin Michel, 2016
[59] J. ARQUILLA & D. RONFELD, *Cyberwar is Coming!*, Comparative Strategy, 1993, pp. 141-165 ;
[60] Discours de M. Le Drian, ministre de la Défense, à Bruz le 12 décembre 2016 ;

Mais la cyberguerre, dans sa définition même, ne concerne finalement qu'un domaine circonscrit à la Défense. Le cyberespace offre d'autre part la possibilité d'engager des manœuvres dans une toute autre dimension, avec des implications bien plus préoccupantes : on parle de netguerres, « *conflits à grande échelle entre nations ou sociétés. Ce qui suppose s'efforcer de changer ou pervertir ce qu'une population cible sait ou croît d'elle-même ou du monde qui l'entoure.* »[61] Les principes et moyens de la cyberguerre s'appliquent de fait, mais la netguerre va bien plus loin dans la mesure où elle s'inscrit dans la manipulation des esprits et des opinions publiques. Il est raisonnable d'imaginer que l'ensemble des organisations dévolues à la cyberguerre versent ou verseront, de près ou de loin, dans la netguerre également. Car, dans toute opération militaire, il s'agit d'abord de porter l'incertitude dans le camp de l'adversaire. Ce principe peut s'appliquer à l'échelle des armées comme des populations. Il ne faut pas abandonner à l'adversaire le terrain des perceptions et c'est en cela que le management de la perception, c'est-à-dire le contrôle de toutes les représentations du réel de l'ennemi ou de la victime, trouve toute sa pertinence. Là où la distribution de tracts, l'instillation de propagandes diverses, les annonces de vérités qui n'en étaient pas, se suffisaient à elles-mêmes dans les conflits anciens, la manipulation de l'information insidieuse et à grande échelle, la perversion de la réalité et la construction finalement d'un truisme virtuel constituent désormais le fondement de la netguerre.

De plus, les dommages occasionnés par les cyberguerres et par les netguerres peuvent impacter directement le monde réel et tangible puisqu'une grande part de l'activité humaine est aujourd'hui fondée sur le cyberespace, dans son assertion la plus large. L'interconnexion des différents réseaux est légion. Dès lors, les dommages collatéraux des actions dans le cyberespace sont difficilement mesurables *a priori*, le « cyber champ de bataille » n'étant pas circonscrit par construction. Les coûts financiers, moraux ou éthiques, infligés à l'adversaire peuvent en conséquence être colossaux et il s'agit donc, pour tout cybercombattant, de ne pas se tromper de cible afin d'éviter des représailles aux conséquences potentiellement non maîtrisables.

Par-dessus tout, il ne faut jamais oublier que les sources de la menace cyber sont éminemment diverses et protéiformes. Pour autant, quels que soient les acteurs de cette menace, les effets obtenus au travers de cyberguerre, de netguerre, ou d' « hacktivisme », peuvent sans nul doute être de même ampleur. Cette situation anxiogène justifie en soi tout l'intérêt porté par l'ensemble des nations et s'inscrit résolument dans la nécessaire agilité des C2.

[61] *Ibid.*

3.1.2. Des informations centrales et pléthoriques

On le voit, l'information est centrale, au cœur des attentions dans le cyberespace. Comme évoqué précédemment, la recherche de la supériorité informationnelle est critique pour toute opération, militaire ou non. Dès lors, les besoins en informations au sein d'un même système C2 vont croissants, ce qui implique une double contingence, au-delà des seules considérations afférentes à la sécurité des systèmes d'information[62]:

- maîtriser le flux d'informations et y discriminer l'information juste et utile ;
- et s'assurer que cette information pertinente est bien connue, comprise et partagée par tous les éléments du C2 qui le nécessitent.

C'est là tout l'art de l'*Information Knowledge Management* (IKM). Pour autant, la notion d'IKM est très peu développée dans les structures militaires françaises, à tout le moins dans son déclinaison la plus pertinente. En effet, bien souvent, la gestion de l'information se limite souvent à celle d'un site en ligne, ou d'une arborescence sur un lecteur réseau partagé. Qui plus est, le personnel en charge de cette gestion n'est le plus souvent pas réellement formé à cette fonction toute particulière. Mais ce qui est le plus problématique dans les armées réside dans ce que sont progressivement devenues les cellules de management de l'information (CMI), censées revêtir l'intégralité des prérogatives inhérentes à l'IKM. En effet, dans l'esprit de bon nombre, la CMI ne constitue qu'un bureau courrier au sens large. Certes, cette fonction est importante, indispensable même, puisqu'elle garantit les bons échanges, les bons référencements et, parfois, les bons archivages de l'information. Pour autant qu'elle soit importante, cette fonction ne répond hélas qu'une toute petite fraction des obligations en matière de maîtrise de l'information, déjà aujourd'hui mais certainement encore plus demain.

En effet, une des contingences consiste à discriminer l'information juste et utile. En aucune façon, une CMI de type bureau courrier n'agit à ce niveau de granularité puisqu'elle s'inscrit résolument en seul gestionnaire du contenant de l'information. Or, pour atteindre un objectif donné, l'accession à temps du contenu pertinent de l'information est une nécessité absolue pour tout chef militaire. Ce besoin d'informations appropriées, illustratif du fonctionnement de tout C2 et fondement de toute prise de décision pertinente, n'est pas nouveau puisque déjà largement décrit au Ve siècle avant Jésus-Christ[63]. L'accroissement des flux, qu'ils soient montants, descendants, voire même transversaux, de plus en plus décloisonnés et partagés, rend le défi de la maîtrise de l'information juste et utile encore plus épineux. Car ce qui

[62] La SSI vise à assurer la confidentialité, l'intégrité et la disponibilité des informations et s'inscrit dans les concepts de cyberdéfense en réponse au cyberespace hostile ;
[63] Sun TZU, *L'Art de la guerre*, Ed. Mille et une nuits, 2000, Article I, pp.7-12;

constitue une information pour l'un ne l'est pas forcément pour un autre, et l'information quant à elle est en réalité noyée dans un océan de données.

Le processus de management de l'information doit donc être en mesure de recueillir les données (*data*), d'en sélectionner les plus pertinentes par une approche cognitive (*capta*) pour ensuite les contextualiser, soit en fonction de la situation soit en fonction des intérêts particuliers, et, *in fine*, produire des faits significatifs qu'il convient alors de dénommer informations. Si les systèmes d'informations pourront certainement prendre à leur charge une partie de ce processus capital mais complexe, ils ne parviendront probablement jamais à abstraire ne serait-ce que les données, à plus forte raison les informations. L'intervention humaine est en conséquence déterminante. Elle l'est d'autant plus que la construction de la connaissance de situation (*situation awareness*), préalable essentiel à la prise de décision, se construit autour de la perception des éléments d'environnement apportés non seulement par les flux continus de communication et de données mais aussi par les retours d'expérience, de la compréhension de la situation actuelle fondée sur les seules informations, puis de l'anticipation des éventuelles conséquences de la décision prise[64].

En conséquence, l'IKM mis en œuvre par les CMI doit couvrir un domaine bien plus important que la seule gestion du courrier. En particulier, la maîtrise de l'information opérationnelle (MI OPS), aujourd'hui très largement orpheline puisque dissoute dans des CMI aux contours déjà inappropriés, doit absolument constituer une priorité. C'est en effet elle qui est garante de flux pertinents d'informations à forte valeur opérationnelle ajoutée, de la capitalisation de ces savoirs fondamentaux pour les opérations en cours ou à venir. Elle doit donc être en place très en amont du déclenchement de quelque opération. En réalité, elle doit être effective en continu car outre le fait qu'elle conditionne nécessairement la physionomie des architectures techniques de transport de l'information, elle permet d'augmenter l'avantage opératif, dès le départ d'une éventuelle opération, dans la mesure où elle participe d'une supériorité informationnelle *a priori*.

[64] Mica R. ENDSLEY, *Toward a Theory of Situation Awareness in Dynamic Systems*, Human Factors, 1995, 37(1), pp.32-64 ;

3.2. L'évolution de l'espace d'affrontements

3.2.1. La numérisation du champ de bataille

Aux niveaux opératif et tactique, et de plus en plus jusqu'au niveau stratégique, les armées mettent en œuvre une palette de systèmes de communications et d'information tendant à répondre à leurs besoins propres, avec la recherche d'une interopérabilité sans cesse accrue. Les réseaux de liaisons de données tactiques (LDT) viennent compléter activement les dispositifs existants, apportant « *un moyen d'échange automatique des informations de données tactiques (position, direction et vitesse des pistes amies ou ennemies, ordres de tir, etc.) entre différentes plateformes des trois armées (aéronefs, bâtiments, centres de défense et coordination surface-air, centres de conduite des opérations aériennes fixes et tactiques, systèmes de détection aéroportée, etc.), unités et états-majors en temps réel ou quasi réel au moyen de systèmes de transmission haut débit, sécurisés et très résistants au brouillage.* »[65] En particulier, les liaisons de données tactiques permettent une remontée des tenues de situation opérationnelle[66] permettant ainsi une construction, une diffusion et un exploitation de la *Common Operational Picture* (COP)[67] par l'ensemble des échelons décisionnels, préalables à toute décision.

En même temps que l'usage des liaisons de données tactiques se généralise, les systèmes de communications se perfectionnent en intégrant progressivement des capacités de traitement d'une information qu'ils sont désormais capables d'extraire des réseaux de données tactiques via les serveurs de données.

C'est pour exploiter la pleine puissance de ces nouveaux outils, que l'Armée de terre s'est par exemple résolument engagée dans le processus de numérisation de l'espace de bataille (NEB) afin de faciliter le processus décisionnel et la conduite de la manœuvre. Ainsi, l'objectif affiché de la NEB réside dans la mise en réseau de l'ensemble des composantes d'une force terrestre engagée en opérations[68], garantissant ainsi, à chacun des acteurs militaires déployés

[65] CICDE, DIA 6_SIC-OPS(2014, les SIC en opérations, 24 juin 2014

[66] CICDE, PIA-3.7_COP(2004) - *Recognized Ground Picture* (RGP), *Recognized Maritime Picture* (RMP), *Recognized Air Picture* (RAP);

[67] L'OTAN utilise désormais davantage l'acronyme CROP (*Common Relevant Operational Picture*) qui désigne l'ensemble des informations pertinentes de la COP ;

[68] Les composantes d'une force terrestre sont au nombre de 24 (Commandement États-majors et techniques d'EM, SIC , Soutien de QG, Renseignement, Géographie Météorologie, Combat embarqué, Combat débarqué, Aérocombat, Génie, Feux indirects, Défense Sol Air, Guerre électronique, Coopération civilo-militaire, Opérations militaires d'influence, Communication opérationnelle, Appui mouvement, Appui à la mobilité des blindés, NRBC, Maîtrise des flux, Maintien en condition des matériels, Soutien du personnel, Soutien au stationnement), réparties dans 8 fonctions opérationnelles (commandement, appui au commandement, renseignement, contact, appui actions sur les perceptions et l'environnement opérationnel, appui à l'engagement,

sur un théâtre ou une manœuvre, le transfert des informations nécessaires d'un bout à l'autre de la chaîne de commandement. Intrinsèquement, elle permet ainsi l'accélération de la boucle décisionnelle de par une facilitation du partage et du décloisonnement de l'information. Malgré les ambitions affichées toutefois, les problématiques demeurent encore nombreuses. En particulier, les niveaux d'exécution tactique peinent à pleinement exploiter les nouvelles possibilités offertes par la NEB tandis qu'elle répond parfaitement aux besoins du niveau opératif dans la conception et la conduite de la manœuvre terrestre. Il y a en effet parfois un décalage entre l'évolution technologique érigée en idéologie et, à la fois, les besoins concrets de l'art de la guerre et les capacités d'utilisation du soldat sur le terrain.[69] Quand on sait que la NEB n'est qu'une étape de l'info-valorisation globale, on comprend toute l'ampleur de l'enjeu. En l'occurrence, le programme SCORPION[70] affiche déjà des ambitions de numérisation et de centralisation à plus grande échelle.

Au-delà du seul cas de la NEB, toutes les composantes marchent à pas forcés vers une numérisation accrue des espaces de combat dans leur milieu d'évolution. Or, même si cette tendance constitue indéniablement un progrès qui s'inscrit résolument dans la modernité et la prise en compte de l'avènement du cyber et de la société en réseaux, elle augmente irrémédiablement la surface de vulnérabilités des forces au combat. En effet, dès lors que les systèmes sont numérisés, interconnectés et centralisés, ils sont davantage sensibles à l'écoute passive, à l'intrusion et à la prise de contrôle. Ainsi, l'automatisation des tirs et liaisons de l'artillerie sol-sol (ATLAS) permet la centralisation de la gestion et la transmission automatique des informations : toute faille de sécurité non couverte et exploitée pourrait neutraliser l'ensemble du système. Cela est d'autant plus problématique qu'au travers du cyber, les attaques peuvent être conduites à tous les niveaux, du plus élevé (humain) au plus bas (matériel).

La numérisation des espaces des champs de batailles demeure malgré tout une tendance irrévocable. Elle revêt de véritables défis qu'il est absolument vital de correctement prendre en compte dans la construction des C2 de demain, que ce soit en termes de sécurisation, d'adaptation aux besoins sur le terrain, de gestion d'une information nécessairement décloisonnée et d'acceptation d'une subsidiarité rendue incontournable ne serait-ce que dans une obligation de résilience aux attaques pouvant paralyser un système.

---

logistique) elles-mêmes cataloguée au sein de 4 fonction IA clés (commander, maîtriser l'information, opérer et soutenir) ;

[69] Joseph HENROTIN, *La technologie militaire en question : le cas américain*, Ed. Economica, 2008, pp. 310-330 ;

[70] Synergie du COntact Renforcée par la Polyvalence et l'Info-valorisatiON ;

3.2.2. Les combattants de demain

Les évolutions technologiques, en partie portées par celles des réseaux, ont permis l'usage de plus en plus marqué de machines visant notamment à éviter à l'homme d'être engagé sous le feu, une tentation possible également de suppléer totalement le facteur huamin dans l'emploi de la force à des fins militaires ou de sécurité. Ce thème suscite un intérêt croissant non seulement pour les pouvoirs publics, mais aussi pour les organisations non gouvernementales les plus influentes dans le domaine de la défense des droits civiques, de l'action humanitaire ou des conflits armés. En particulier, des débats vifs sont en cours concernant l'immixtion grandissante des drones et des robots sur le champ de bataille, à l'image de ceux nés de l'intégration du progrès technologiques dans les sociétés tout au long de l'histoire des sciences et des techniques et de l'histoire sociale. Pour s'en convaincre, il suffit de se rappeler les gesticulations et les conflits nés de l'introduction des machines dans l'outil de production ou encore de l'arme atomique dans l'univers des conflits armés. Au-delà des machines, le citoyen devient aussi progressivement un combattant à l'ère numérique. Quoi qu'il en soit, ces nouveaux combattants sont désormais une réalité grandissante.

3.2.2.1. Les drones

Un drone ou RPAS (*Remotely piloted aircraft systems*[71]) est un aéronef inhabité, piloté à distance, semi-autonome ou autonome, susceptible d'emporter différentes charges utiles le rendant capable d'effectuer des tâches spécifiques pendant une durée de vol pouvant varier en fonction de ses capacités. Malgré cette définition somme toute aéronautique, il existe également des drones marins, sous-marins et terrestres.

La plupart des drones aériens ne sont pas armés et sont utilisés pour des actions de renseignement, en particulier pour « *la surveillance persistante d'une cible et de son environnement, en complément d'autres moyens (avions légers de surveillance et de renseignement, satellite, etc.)* »[72]. L'utilisation de la FMV (*full motion video*), supportée par la puissance des réseaux, permet une diffusion des informations captées, sûre, continue et quasi instantanée, potentiellement à tout organe le nécessitant. Les drones armés actuels sont des drones de surveillance classiques, équipés de missiles à dessein d'être en mesure de réaliser en vol l'intégralité du cycle de ciblage[73]. Pour la très grande majorité d'entre eux, ils sont

[71] Contrairement à la traditionnelle définition UAV (*unmanned aerial vehicle*) qui ne concerne que l'aéronef lui-même, un RPAS regroupe l'aéronef, le cockpit, l'équipage -au sol-, les liaisons de données, les charges utiles ;
[72] Jean-Baptiste JEANGENE VILMER et Christophe FONTAINE, *Drones armés, drones de combats et « robots tueurs »*, www.theconversation.com, 2016, consulté le 11/02/2017;
[73] Détection, identification, poursuite, analyse des risques de dommages collatéraux, guidage de l'armement, analyse du résultat ;

lents, non furtifs et peu manœuvrants et ne sont donc utilisables que dans des milieux permissifs. On parle ici des drones MALE[74], tel que le MQ-9 Reaper. Très prochainement, apparaîtront des drones de combats utilisables en milieux non-permissifs visant à corriger les vulnérabilités inhérentes aux menaces air-air ou sol-air. Les démonstrateurs français Neuron et britannique Taranis augurent déjà du projet commun de système de combat aérien futur (SCAF) qui entrera vraisemblablement en concurrence avec les projets américains et chinois.

Cela étant, en quoi les drones sont-ils un enjeu en matière de C2 ? Contrairement aux idées souvent reçues, l'homme est constamment présent dans l'usage de ces drones, y compris armés. « *La cible est choisie par le commandement et, le moment venu, c'est le pilote qui tire, exactement comme s'il était dans un avion ou un hélicoptère.* »[75] En réalité, la différence fonctionnelle majeure avec un aéronef classique réside dans le fait que le cockpit est déporté au sol. Par ailleurs, ce qui impacte réellement le C2, c'est la précision et l'endurance de ces capteurs de renseignements : tous les niveaux hiérarchiques sont désormais gourmands des images transmises par les drones, tant et si bien qu'ils investissent toutes les sphères de sécurité, et pas seulement militaires. Il faut donc disposer non seulement de canaux de communications à la hauteur des capacités des drones, en termes de résilience et de débits, mais aussi de systèmes d'information capables de traiter cette multiplication d'informations émanant de drones de tous types et de plus en plus nombreux. Enfin, les flux vidéo étant souvent distribués à tous les échelons, la tentation est alors grande pour l'échelon le plus élevé de s'immiscer dans la décision relevant du plus bas, compromettant la nécessaire subsidiarité. Cela est accentué par le fait que les drones constituent dorénavant un outil au service du politique. Pour illustrer cette tendance, comment ne pas penser à la politique étrangère, au travers des assassinats ciblés, menée par les Etats-Unis en Afghanistan, au Yemen ou plus généralement dans le Moyen-Orient.

3.2.2.2. Les robots

Outre les drones, d'autres acteurs font leur apparition : les robots-tueurs ou « *killer robots* ».

Pour rappel, le robot est un dispositif mécatronique[76]conçu pour accomplir automatiquement des tâches imitant ou reproduisant, dans un domaine précis, des actions humaines. Pour ce qui concerne les différents théâtres tant militaires que sécuritaires, on parle de systèmes d'armes létaux autonomes (SALA). Il s'agit de robots de terrain, « *des systèmes d'armes qui, une fois*

[74] Moyenne altitude, longue endurance ;
[75] Jean-Baptiste JEANGENE VILMER et Christophe FONTAINE, *Drones armés, drones de combats et « robots tueurs »*, www.theconversation.com, 2016, consulté le 11/02/2017;
[76] Dispositif alliant mécanique, électronique et informatique ;

activés, seraient capables de sélectionner et d'éliminer des cibles sans intervention humaine »[77] Ce sont eux qui font le plus débat dans la communauté internationale et, bien qu'ils ne soient encore qu'à l'état de projet le plus souvent, une réunion annuelle se tient à l'ONU à leur sujet depuis 2014. Leur autonomie de décision pose le plus de questions, surtout lorsqu'il s'agit de donner la mort. Car, sur le plan du droit, l'autonomie de la volonté est l'une des prérogatives de la personne juridique, ce qui fonde la différence entre la personne et le bien, le sujet et l'objet de droit. Si le progrès technique est susceptible de déboucher sur des machines disposant d'une autonomie de ce type, les frontières actuelles entre l'homme est la machine se brouillent. De plus, comment engager quelque responsabilité en cas de dommages collatéraux que la législation et la morale réprouveraient ? La machine n'est aujourd'hui qu'un objet et doit le rester. Il serait hasardeux de conférer une personnalité juridique, même partielle, à ce qui, techniquement, s'analyse comme un objet de droit et non comme un sujet de droit.

Quoi qu'il en soit, il n'est probablement pas envisageable que l'homme soit totalement exclu de l'engagement de ces robots autonomes ou partiellement autonomes. En effet, il paraît essentiel qu'un système de réversibilité à la décision menant à l'action létale, voire de reprise de contrôle total du SALA, soit en place afin d'éviter toute manœuvre non souhaitable, qu'elle soit liée à une mauvaise estimation du robot, d'une attaque virale malintentionnée ou, tout simplement, d'une défaillance du système. De même, il ne saurait non plus être envisageable d'avoir des robots-tueurs en totale libre circulation. Ces dernières conditions, *a minima*, conduisent à la nécessité d'avoir un système C2 encore plus performant, probablement encore plus interconnecté et donc encore plus sensible aux attaques.

3.2.2.3. Le citoyen

Le citoyen se sent de moins en moins sécurité. Les forces armées sont, pour l'essentiel, engagées sur les théâtres d'opérations extérieures, tandis que les forces de sécurité intérieure sont de plus en plus militarisées. Dans le même temps, les budgets de défense, en particulier européens, ont longtemps stagné voire régressé alors que le monde entier se réarmait et que l'instabilité allait grandissante. Le citoyen se sent de plus en plus concerné par sa sécurité, par la sécurité de son environnement. On assiste donc parfois à une « privatisation » de la sécurité, reprise en mains par le citoyen au travers de formes d'organisations en marge de toute structure étatique. En outre, cela « *permet de répondre au changement d'échelle de l'équilibre de la terreur* […] *rendant à la légitime défense sa signification première, c'est-à-*

[77] Jean-Baptiste JEANGENE VILMER et Christophe FONTAINE, *Drones armés, drones de combats et « robots tueurs »*, www.theconversation.com, 2016, consulté le 11/02/2017;

dire le droit fondamental d'un individu de garantir sa vie, ses biens et sa propriété en cas de défaillance de l'Etat. »[78]

En l'occurrence, les nouveaux moyens d'actions offerts par l'utilisation de plus en plus banalisée du réseau de réseaux, permettent au citoyen de mettre ses talents au service de communautés. Bien évidemment, les organisations terroristes ont tôt fait de s'approprier cette dimension d'actions nouvelles. Pour autant toutes les intentions du citoyen ne sont pas mauvaises, pour peu qu'elles s'expriment dans une dimension noble de protection de biens communs à la communauté. Cela constitue une réalité avec laquelle il faut composer, d'autant plus que le citoyen peut être manipulé par un récit communautaire biaisé ou encore qu'il ne maîtrise pas les entiers dommages collatéraux qu'une action pourrait avoir dans un système totalement interconnecté.

3.3. Le commandement 3.0

Jusqu'à la fin du XVIIIe siècle, le chef d'armée avait l'exclusivité de la conception et un quasi-monopole de la conduite des opérations militaires. La mise en application du principe divisionnaire, en même temps que les évolutions en termes d'armements, d'infrastructures et de systèmes de communications, a entraîné une dilution des dispositifs et une métamorphose des organisations. Progressivement, tous les niveaux sont ainsi amenés à concevoir la manœuvre et à participer à son exécution. « *Cette pratique n'est plus viable, car l'ampleur des tâches correspondant à chacune des fonctions est devenue telle, que la dispersion de l'effort sur les trois en arrive à compromettre le résultat de chacune.* […] *Il faut arrêter de vouloir tout faire à la fois, et consacrer un échelon de commandement au suivi des engagements, à la gestion de l'information et à la coordination des moyens*.»[79]

3.3.1. La structure organique

Comme énoncé précédemment, en réponse aux évolutions liées à l'avènement de l'ère de l'information et à l'émergence de nouvelles considérations propres au cyber, les structures organisationnelles devront être moins pyramidales et plus hybrides. L'initiative personnelle et la subsidiarité seront nécessaires. Mais toutes deux ne sont envisageables dans une organisation de type militaire qu'à la condition que le cadre global d'actions en a été fixé au préalable. Il ne s'agit donc nullement d'imaginer une structure organique qui verserait dans

[78] Bernard WICHT, *Europe Mad Mac demain ? Retour à la defense citoyenne*, Ed.Favre, Lausanne, 2013, pp 131-144;
[79] Guy HUBIN, *Perspectives tactiques*, Ed. Economica, Paris, 2009, pp.71-80;

l'anarchie, sans chef aux commandes. La métamorphose qui s'impose ne porte pas sur l'existence même de structures de commandement, mais bien sur les méthodes d'exercice de ce commandement.

« *Généralement, le commandement du grand nombre est le même que le petit nombre, ce n'est qu'une question d'organisation. Contrôler le grand et le petit nombre n'est qu'une seule et même chose, ce n'est qu'une question de formation et de transmission des signaux* »[80] L'unicité de commandement est donc toujours primordiale. Cela est encore plus pertinent lorsqu'on se penche sur le domaine du cyber, à la fois potentiel espace d'opérations propres et fondement essentiel pour les manœuvres dans les autres milieux traditionnels.

En ce sens, les discours du ministre de la Défense visant la création d'un commandement propre au cyber trouvent toute leur justification. Néanmoins, les évolutions demeurent encore timides. Les organisations militaires ont ceci de particulier qu'elles sont rétives aux transformations, dès lors qu'elles sous-tendraient une perte de compétence d'armée, ne serait-ce même que ressentie et donc non fondée, dès lors qu'il s'agirait en conséquence de ne plus seulement imaginer le commandement autrement que selon une logique de milieu. Or les contingences du monde et des opérations à venir imposent résolument de dépasser ces réticences d'un autre âge. En effet, le CYBERCOM ne devrait être qu'un préalable en tant que tel. L'unicité de commandement vaut quel que soit l'environnement considéré. Ainsi, pour obtenir le meilleur résultat dans l'espace cyber et ainsi constituer une assise solide pour les opérations dans les autres milieux, il paraît indispensable que ce commandement prenne pied sur l'ensemble des couches caractéristiques du cyber. L'exploitation de la seule couche cognitive ne devrait être en ce sens qu'un préalable, et la coordination des actions dans les couches physiques et logiques paraît indispensable. Dit autrement, le CYBERCOM, pour être totalement efficace, devrait englober à terme toutes les structures d'armée ou interarmées aujourd'hui consacrées aux systèmes d'information et de communication. Le domaine des SIC et du cyber sont encore aujourd'hui artificiellement dissociés, du fait des résistances du premier et de l'immaturité du second. La création d'une quatrième armée paraît subséquemment incontournable, non pas seulement selon une logique de milieu mais bien pour un gain substantiel d'efficacité globale des C2 dans tous les milieux.

En parallèle, même si les évolutions technologiques apportent des interfaces homme-machine de plus en plus intuitives, il ne faut pas imaginer que la mise en œuvre des outils opératifs modernes reste et restera à la portée du premier venu. Il y a un réel besoin de formation et

[80] Sun TZU, *L'Art de la guerre*, Ed. Mille et une nuits, 2000, article V, pp. 29-33 ;

d'entraînement, encore plus accru face aux systèmes de combat modernes, qu'il s'agisse d'une part de pleinement appréhender les entières capacités de ces systèmes et d'autre part d'obtenir l'adhésion de l'ensemble des niveaux de conception et de conduite. Cela est vrai également dans le domaine des SIC et du cyber. Une même structure organique chapeautant ces deux domaines donnera substance et consistance à l'acquisition d'un niveau technique compatible avec les menaces d'un monde changeant, au travers de formations et d'entraînements dédiés. Pour ne s'intéresser qu'aux forces consacrées aux SIC aujourd'hui, force est de constater qu'elles ne s'entraînent que très rarement : elles participent certes évidemment aux divers exercices, non pas pour s'entraîner mais bel et bien pour fournir les moyens C2 aux autres composantes participant, elles, pleinement aux exercices en question. Les forces SIC sont donc continuellement en opérations et l'intégration des nouveaux systèmes dans les architectures est très souvent réalisée directement sur le terrain.

Plus généralement, les structures de commandement sur le terrain devront être adaptatives et reconfigurables. En effet, comme évoqué, flexibilité et adaptation constituent des prérequis fondamentaux à l'agilité des C2. Ces derniers doivent être en mesure de s'ajuster à la menace et à la réponse de l'adversaire qui leur sont opposées, au tempo des opérations qui peut notoirement évoluer au fil de l'exécution de la manœuvre, voire des changements d'orientation de l'échelon politique. En la matière, une structure organique par trop rigide serait inadaptée car, par construction, ses processus de fonctionnement seraient trop figés pour pouvoir s'adapter à temps à quelque bouleversement inattendu.

3.3.2. La prise de décision

La prise de décision est au cœur de tout C2. En première approche, le chef est considéré comme l'autorité ayant seule légitimité à prendre ces décisions. En réalité, il délègue usuellement cette autorité à de nombreux autres acteurs dont les décisions sont du reste souvent importantes. Ces acteurs ne sont pas toujours des individus, dont l'autorité est directement liée à leur positionnement hiérarchique, mais sont aussi quelquefois des comités ou des groupes à la physionomie et à l'assise décisionnelle variées. En toute rigueur, la délégation du pouvoir de décision[81] pourra certainement devenir la règle, cela étant facilité par les nouvelles technologies inhérentes à l'avènement de l'ère de l'information. Quoi qu'il en soit, les systèmes C2 devront, selon toute évidence, non plus seulement assister le chef dans sa prise de décision, mais plutôt assister et faciliter l'appréciation et le jugement

[81] http://www.maitre-couturier.com/pdf/Delegation-de-pouvoirs.pdf, consulté le 18/02/2017 ;

humains, à différents niveaux de responsabilités, sans jamais toutefois les supplanter. Afin d'y parvenir, ces systèmes C2 futurs devront répondre à un certain nombre d'exigences.

Tout d'abord, les systèmes C2 devront être en mesure d'assister plus efficacement le décisionnaire, délégué ou pas, dans des modes d'action à la fois proactif et réactif. En effet, lorsqu'il a l'initiative, il doit être en mesure d'influencer le déroulement des opérations de sorte à forcer l'ennemi à réagir. *A contrario,* si l'initiative n'est plus possible ou en cas de « *marche à l'ennemi* »[82], il doit toujours être capable de réagir avec efficacité à toute action de l'ennemi, qui plus est lorsque le brouillard de la guerre s'épaissit avec l'ère de l'information.

Par ailleurs, la rapidité dans la prise de décision est un élément fondamental dans la conduite des opérations. Moins le décisionnaire prendra de temps à orienter les actions, plus ses subordonnés pourront effectivement intégrer ces décisions, planifier les opérations en découlant et les exécuter avec efficacité. Ainsi, dans un mode de prise de décision proactive, le facteur temps est de plus absolument déterminant puisqu'il permet au chef de conserver l'avantage sur l'adversaire et de maintenir ce dernier dans un mode réactif, jusqu'à son essoufflement. Dans un mode réactif, la rapidité de décision permet au décisionnaire de reprendre éventuellement l'avantage sur l'adversaire, *a minima* de réagir au mieux à ses actions afin d'en limiter l'impact sur le déroulement globale des opérations. C'est donc la prise de décision qui détermine le rythme des opérations et, subséquemment, la supériorité sur l'ennemi.

Toutefois, cela n'est vérifiable qu'à la condition que les décisions prises soient les bonnes. L'histoire militaire est jalonnée de maints exemples de mauvaises décisions prises trop rapidement ou de bonnes décisions arrivées trop tard. L'essence du commandement, plus particulièrement au combat, réside dans l'art de trouver le juste équilibre entre vitesse de prise de décision et qualité de ces décisions et c'est là que les systèmes C2 trouvent toute leur pertinence. Tout système participant de l'aide à la décision doit en effet être en mesure de faciliter la détermination de la chronologie des points de décision, lorsque ces derniers doivent impérativement intervenir, qu'ils soient dictés par l'urgence en réaction ou par l'intention en proactivité. Il devrait être également être capable de mesurer la qualité des décisions prises, même si ceci est loin de constituer une gageure, car cela répond à deux exigences essentielles du commandement : apprendre des succès et des échecs, et s'y adapter.

[82] On parle de "marche à l'ennemi", en référence à l'un des concepts de Sun Tzu dans l'*Art de la Guerre* (exemple de l'eau, dans le chapitre 6) et développé par Michel Yakovleff dans son ouvrage *Tactique théorique* (partie 4.2), lorsque la manœuvre n'étant pas encore décidée au moment du contact avec l'adversaire, celle-ci s'élabore en conduite et en réaction à celle de l'ennemi ;

En d'autres termes, il doit faciliter l'élaboration du retour d'expériences (RETEX) à dessein d'accélérer les boucles de décisions ultérieures, en gageant de leur qualité toujours plus pertinente à la lumière des corrections incrémentielles que cette activité sous-tend.

Enfin, l'ISR[83]trouve toute sa place dans le processus de prise de décision dans la mesure où il influe directement à la fois sur sa rapidité et sa qualité. La recherche du renseignement, et plus généralement l'ISR, constitue donc un enjeu majeur pour tout C2, ce qui est illustré notamment par l'usage croissant de capteurs de plus en plus performants. Qu'il s'agisse de drones, d'avions ou de capteurs humains, l'intégration des flux ISR dans le processus C2 doit constamment être recherchée.

3.3.3. L'exécution

La phase d'exécution se réfère en réalité à celle correspondant à la conduite des opérations. La confrontation sur le champ de bataille, la résistance de l'adversaire et les évolutions de l'environnement sont autant de facteurs qui conduisent à la révision des plans initiaux ne résistant pas aux premiers échanges, comme le sous-tendait Von Moltke. Carl Von Clausewitz parlait de « *friction* »[84] en référence à la multitude d'éléments constitutifs de l'art de la guerre qui, combinés entre eux, amènent à reporter une opération, à la repenser voire même la mettre à plat. Dès lors, à mesure du déroulement d'une opération, le commandant s'efforce d'évaluer son évolution en temps réel et d'énoncer des ordres rapides et clairs à dessein d'atteindre ses objectifs.

Généralement, la phase d'exécution procède de l'intégration de trois fonctions principales du C2: la connaissance de situation, la planification et la prise de décision. On pourrait, à tort, considérer que chacune de ces fonctions découle de l'autre de façon séquentielle : la connaissance de situation permet la planification, la planification nourrit la prise de décision, et l'action résultant de la prise de décision conduit à une modification de l'environnement, ou de l'état du système adverse, modification qui permet un affinement de la connaissance de situation. Selon toute évidence, ces trois fonctions sont mises en jeu simultanément, d'autant plus que leur intégration va *crescendo* au fur et à mesure de l'intensification de l'action. En fait, la connaissance de situation révèle continuellement l'état d'avancement de la campagne et de l'exécution de la planification, mettant au jour les éventuelles mises à jour ou des prises de décisions qui s'imposeraient. De plus, aux fins d'anticipation, planification et prise de décision se concentrent, activement et simultanément, sur tous les moyens aboutissant à la

[83] *Intelligence, surveillance and reconnaissance ;*
[84] Carl Von CLAUSEWITZ, *On war*, Princeton University Press, Princenton 1976, p119 ;

connaissance de situation, qu'il s'agisse d'orienter la recherche du renseignement, d'évaluer les dommages opérés sur une cible, de mesurer les capacités résiduelles, tant de la force commandée que de l'adversaire, etc. Dans ces conditions, ces trois fonctions contribuent à la réactivité nécessaire en conduite, alliant subtilement l'utilisation de l'information à temps, la collaboration, la rapidité et la qualité de la prise de décision.

Qu'il s'agisse d'organisation, de prise de décisions ou d'exécution, le principe de « *leading from behind* »[85] devient de plus en plus pratiqué, grâce notamment aux évolutions technologiques en matière de systèmes de communications et d'information. C'est ainsi notamment que les opérations aériennes en Afrique sont d'ores et déjà conduites depuis un JFAC AFCO basé à Lyon Mont Verdun, que les flux vidéo émanant des différents drones peuvent être diffusés à tous les échelons. Mais la délocalisation a inévitablement ses limites, les relations humaines directes conditionnant la réussite des opérations, car ces opérations demeurent d'abord et avant tout des aventures humaines. En conséquence, bien que le principe de « *leading from behind* », combiné à l'infovalorisation, trouve toute leur pertinence, un échelon de coordination au plus près du terrain d'affrontements s'avère nécessaire. En ce sens, la notion de C2 mobile et projetable restera, quoi qu'il en soit, incontournable.

*

* *

[85] Philippe GROS, *« Leading from behind » : contour et importance de l'engagement américain en Lybie*, Politique américaine, 1/2012 (n°19), Ed. L'Harmattan, 2012, p.49-68 ;

Conclusion

L'environnement global des opérations s'est considérablement métamorphosé. Sans qu'il soit question de rupture, les mutations nées de ces changements sont profondes. En effet, la circulation facilitée, voire presqu'instantanée de l'information étant immanente à l'usage, à l'interconnexion et aux performances galopants des réseaux, chaque élément connecté au réseau de réseaux est devenu un capteur, un émetteur, un transmetteur perpétuel et instantané d'une information qui devient quasiment impossible à appréhender dans sa globalité.

Dès lors, la maîtrise de l'information relève d'un défi majeur pour la conception, la planification, le commandement et la conduite des opérations militaires car d'elle naît la faculté de connaître la situation et d'anticiper les réactions adverses. D'elle naît la capacité fondamentale de porter l'incertitude chez un adversaire qui, potentiellement, a les mêmes capacités et vise les mêmes buts. Finalement, de la maîtrise de l'information dépend l'avantage opératif et la recherche de la suprématie informationnelle constitue alors un objectif décisif.

Néanmoins, cet objectif est d'autant plus délicat à atteindre que les processus et les organisations en place actuellement demeurent immatures en regard de l'ampleur des défis à surmonter. Cette constatation est d'autant plus pertinente que la France, habituée à une forme de gestion jacobine et colbertiste a des difficultés à s'adapter à la société en réseaux, et que cela vaut également, dans une certaine mesure, pour les armées. Alors que « les défis sont la maîtrise du tempo opérationnel, la capacité à distribuer les effets simultanément, celle à agir sur les perceptions, l'efficacité de l'action face à l'asymétrie, les interopérabilités et l'innovation. »[86], les enjeux sont de différentes natures.

Tout d'abord, il s'agit de faire face à l'altération de la perception du temps et de l'espace. En réalité, l'espace a en quelque sorte pris sa revanche sur le temps : tandis qu'autrefois le temps qui façonnait l'espace, aujourd'hui, c'est l'inverse de par l'instantanéité des échanges. Pour autant, tous deux se sont eux-mêmes contractés. Les élongations spatiales ne sont plus aussi importantes pour le C2 que par le passé, alors que, concomitamment, le tempo des opérations

[86] http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415026.asp, consulté le 28/02/2017.

s’accélère du fait de l’apport technologique en matière de communications et de traitement de l’information.

Ensuite, nous assistons à un aplatissement et à une porosité grandissante de l’organisation pyramidale et structurée, pourtant traditionnellement si chère aux militaires. En effet, d’une part, à la verticalité des hiérarchies a succédé l’horizontalité des échanges, consubstantielle à la mise en avant d’une organisation davantage en réseau, plus plate, voire holacratique. Une subsidiarité davantage assumée est ainsi devenue essentielle aux C2 afin de garantir une prise de décision efficace et opportune dans un environnement devenu plus complexe, plus insaisissable, plus incertain aussi. L’hybridation des conflits actuels et certainement encore davantage ceux de demain n’y est pas étrangère puisqu’à présent l’utilisation, en permanence et par tous les acteurs, de l’ensemble des possibilités offertes dans tous les domaines, notamment en exploitant le champ informationnel, est une réalité avec laquelle il faut composer. D’autre part, dans le même temps, la compression des niveaux stratégique, opératif et tactique jusqu’alors bien définis et délimités, apparaît inexorable, toujours sous l’influence de l’accélération croissante du tempo opérationnel.

En conclusion, le monde de plus connecté conduit à une refonte de la conception et de l’organisation de nos C2 puisqu’il s’agit tout à la fois d’appréhender un temps devenu intemporel, de prendre en compte un espace désormais infini, de maîtriser une information aujourd’hui universelle, pléthorique et instantanée, d’intégrer de nouveaux acteurs dans le champ des affrontements, d’assumer une organisation plus plate, modulaire et transversale tout en renforçant et en encadrant une subsidiarité incontournable. L’hybridité des conflits n’est en soi pas une nouveauté, elle est un facteur multiplicatif des enjeux dans la mesure où les armées, habituées aux modes d’action cinétiques et aux affrontements entre forces déterminées, doivent à présent reconstruire des capacités diversifiées prenant appui en particulier sur l’environnement civil, un environnement résolument interconnecté et potentiellement hostile.

Références

Publications de portée générale

1. David S. ALBERTS, *The unintended consequences of information age technologies*, Ed. University press of the Pacific, 2004
2. J. ARQUILLA & D. RONFELD, *Cyberwar is Coming!*, Comparative Strategy, 1993
3. Christophe BARTHELEMY, *La judiciarisation des opérations militaires*, Thémis et Athéna, Ed. L'Harmattan, 2013
4. Aymeric BONNEMAISON et Stéphane DOSSE, *Attention : cyber ! Vers le combat cyber-électronique*, Ed. Economica, Paris, 2014
5. Manuel CASTELLS, *La société en réseau - L'ère de l'Information*, Ed. Fayard, Paris, 1998
6. Tom CLANCY, *Cybermenace*, Ed. Albin Michel, 2016
7. Carl Von CLAUSEWITZ, *On war*, Princeton University Press, Princenton, 1976
8. Marc ELSBERG, *Black Out – Demain il sera trop tard*, Ed. Piranha, 2016 (2e édition)
9. Mica R. ENDSLEY, *Toward a Theory of Situation Awareness in Dynamic Systems*, Human Factors, 1995
10. Pierre GOETZ et Olivia CAHUZAC-SOAVE, *Impact de la numérisation sur l'exercice du commandement*, Les notes stratégiques, CEIS, décembre 2015
11. Tiphaine GRALL, *La numérisation dans les Armées : similitudes et disparités des doctrines nationales*, Doctrine n°14, janvier 2007
12. Philippe GROS, *« Leading from behind » : contour et inmportance de l'engagement américain en Lybie*, Politique américaine, Ed. L'Harmattan, 1/2012 (n°19), 2012
13. Joseph HENROTIN, *La technologie militaire en question : le cas américain*, Ed. Economica, Paris, 2008
14. Guy HUBIN, *Perspectives tactiques*, Ed. Economica, Paris, 2009
15. Francis JAUREGUIBERRY et Jocelyn LACHANCE, *Le voyageur hypermoderne – partir dans un monde connecté*, Ed. Erès, 2016
16. David POTTS, *Command and combat in the information age : the big issue*, Ed. Pavillon Pr Inc, 2004
17. Kavé SALAMATIAN et Jérémy ROBINE, *Peut-on penser une cybergéographie ?*, Revue Hérodote, 2014/1-2 (n°152-153)
18. Sun TZU, *L'Art de la guerre*, Ed. Mille et une nuits, 2000
19. Bernard WICHT, *Europe Mad Mac demain ? Retour à la defense citoyenne*, Ed. Favre, Lausanne, 2013
20. Michel YAKOVLEFF, *Tactique théorique*, Ed. Economica, Paris, 2016 (3e édition)

Publications du CICDE

1. CIA 01, *Concept d'emploi des forces*, 15 janvier 2010
2. CIA-6.3 *Cyberdéfense*, 12 juillet 2011
3. DIA-01(A)1_DEF(2014), *doctrine d'emploi des forces*, 12 juin 2014
4. DIA-3(A)1_CEO(2014), *commandement des engagements opérationnel*, 24 juin 2014
5. DIA-3.20_CYBER(2014), *Cyberdéfense*, 28 mars 2014 amendée le 21 juin 2016
6. DIA 6, *Les SIC en opérations*, 24 juin 2014 amendée le 16 janvier 2016
7. PIA-3.7_COP(2004), *Common operational picture*, 2004
8. PIA-3.9.9_EDC(2014), *Estimation des dommages collatéraux*, 2 juillet 2014

Sites internet consultés

1. http://www.assemblee-nationale.fr
2. http://www.theconversation.com
3. http://www.institut-montalembert.fr/
4. http://www.dioceseauxarmées.fr
5. http://www.huyghe.fr
6. http://www.halshs.archives-ouvertes.fr
7. http://www.lejdd.fr
8. http://www.lemonde.fr
9. http://www.lci.fr/
10. http://www.air-cosmos.com
11. https://www.information-security.fr/
12. http://www.maitre-couturier.com/