ceis

Numérisation de l'Outil de Défense

Des impacts multiples sur les moyens, les compétences et la formation

Par Asinetta Serban et le GB (2S) Christian Cosquer

Juin 2015

Les notes σtratégiques

Les notes stratégiques

Policy Papers – Research Papers

Les auteurs souhaitent remercier l'ensemble des experts rencontrés au cours de cette étude.

Les idées et opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de CEIS ou des experts rencontrés.

CEIS est une société de conseil en stratégie.

Notre vocation est d'assister nos clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, nous associons systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action.

L'activité Défense et Sécurité de CEIS regroupe les expertises sectorielles et activités de CEIS dans ce domaine. La vingtaine de consultants et d'analystes du secteur Défense et Sécurité disposent d'un réseau international de plusieurs centaines d'experts et d'organisations.

Implanté à Bruxelles, le Bureau Européen de CEIS conseille et assiste les acteurs publics, européens ou nationaux, ainsi que les acteurs privés dans l'élaboration de leur stratégie européenne, notamment sur les problématiques de défense, sécurité, transport, énergie et affaires maritimes. CEIS - Bureau Européen participe également à des projets de recherche européens dans ces domaines. Pour mener à bien l'ensemble de ses missions, l'équipe s'appuie sur un réseau européen de contacts, d'experts et de partenaires.

Le SIA Lab est mis en œuvre et animé par CEIS qui agit sous la responsabilité de l'Architecte Intégrateur du SIA (Système d'information des Armées), la société SOPRA Group. Ce concept innovant de la Direction Générale de l'Armement a pour objectif de détecter, expérimenter, et démontrer des briques technologiques sur étagère ou

susceptibles d'être fournies par des PME/PMI innovantes ou des industriels.

Le SIA Lab vise à rapprocher les utilisateurs et concepteurs du Système d'Information des Armées (SIA) des potentiels fournisseurs de solutions, qu'ils soient industriels ou étatiques. C'est également un espace de réflexion et de discussion visant à cerner au mieux les besoins des utilisateurs et l'adéquation des solutions présentées.

Contact : CEIS
Défense & Sécurité
Axel Dyèvre – Directeur
adyevre@ceis.eu

Défense & Sécurité	***Bureau Européen***	***SIA Lab***
280, boulevard Saint Germain	Boulevard Charlemagne, 42	40, rue d'Oradour-sur-Glâne
F-75007 Paris	B-1000 Bruxelles	F-75015 Paris
+33 1 45 55 00 20	+32 2 646 70 43	+33 1 84 17 82 77

www.ceis.eu www.sia-lab.fr

SOMMAIRE

Synthèse

"We're going to be in an environment in this new world where so much is digitalised that both state and non-state actors are going to have the capacity to disrupt our lives in all sorts of ways"

(Barack Obama – 2014)

En une ou deux décennies, la numérisation s'est progressivement imposée à tous les niveaux du quotidien de nos sociétés: activités sociales, activités professionnelles, relations familiales. Musique, téléphone, médias, livres, cartes géographiques, monnaies virtuelles, tickets de transport, livret médical sont devenus autant de biens numériques en l'espace de quelques années, bouleversant des industries établies. Mais Internet n'est plus seulement un moyen de communication, de divertissement, et de commerce. Il est devenu un système critique pour la survie économique des entreprises et pour le fonctionnement des infrastructures vitales (énergie, transport, santé, alimentaire) et de la société en général.

La numérisation a également des implications profondes pour l'outil de Défense, que ce soit dans le fonctionnement courant des forces armées ou dans la conduite des opérations. Elle permet un raccourcissement généralisé des

boucles informationnelles et décisionnelles et une réactivité accrue des forces. Ce phénomène, si l'on n'y prête pas attention, pourrait avoir comme conséquence un écrasement des chaînes hiérarchiques. Elle implique aussi une technicité accrue dans les moyens mis en œuvre et leur cyber protection et donc un besoin de profils plus techniques. Enfin, en termes d'usages, la société dans laquelle les forces armées évoluent étant hyper connectée, elles sont confrontées à une surexposition médiatique rendant les populations plus sensibles aux actions des forces armées – même à distance.

La liste de ces changements plus ou moins amorcés pourrait être continuée quasiment à l'infini : l'utilisation des réseaux sociaux pour une communication en tout temps et en tout lieu, la multiplication des objets connectés pour des applications liées à la santé, l'utilisation de robots ou de véhicules autonomes sont autant d'exemples de l'omniprésence du numérique. Et tous ont un impact sur le fonctionnement des forces armées.

Une des conséquences de ces nouveaux usages numériques est le sentiment de l'effacement de la frontière entre mondes civil et militaire, entre sécurité et défense et entre sphères publique et privée. D'une complexité croissante, tous les équipements sont appelés à évoluer de façon de plus en plus connectée et interdépendante.
Mais au delà des systèmes d'armes et des équipements, l'action militaire est l'expression d'une volonté où la place de

l'homme est centrale. Clausewitz disait que « la guerre est la continuation de la politique par d'autres moyens ». C'est pour cette raison essentielle qu'il s'agit de garder les hommes au cœur de la réflexion sur les impacts de ces changements en cours. Ceux-ci doivent être pris en compte en adaptant la préparation opérationnelle et le modèle des ressources humaines tout en assurant la cohérence opérationnelle et organique.

Numérisation et communication

Les ordinateurs, smartphones et tablettes donnent accès à de multiples applications de communication - Skype, Whatsapp, Twitter, Facebook, Snapchat, Instagram - qui permettent à tout un chacun de communiquer avec le monde entier à partir d'une simple connexion à un réseau.

On estime d'ailleurs qu'en 2025, 80% des connections à Internet seront en effet faites à partir de terminaux mobiles[1], Internet et les réseaux sociaux représentent aux yeux de tous la liberté de s'exprimer sans passer par les relais habituels de communication. Ils permettent l'interactivité, la discussion et l'échange mais échappent à tout contrôle aussi bien pour l'accès que pour la diffusion des contenus. De nombreux militaires utilisent maintenant les réseaux sociaux à titre privé depuis les théâtres d'opération. Ils peuvent passer par les infrastructures mises à leur disposition par les Armées, ou acheter sur place des téléphones ou abonnement. Ces médias leurs permettent de garder le contact avec leurs proches, de « skyper » leur famille ou de garder le lien avec leur communauté sur Facebook. Mais ils ont également la possibilité de transmettre de manière plus ou moins volontaire des informations qui peuvent se révéler sensibles : l'armée anglaise a enquêté ainsi sur un certain nombre de cas, comme par exemple la diffusion d'informations sur le

[1] http://www.mckinsey.com/insights/business_technology/disruptive_technologies

fonctionnement de bases en Afghanistan, avec les horaires des patrouilles[2].

L'irruption depuis quelques années des appareils mobiles personnels soulève– et va soulever de plus en plus – de multiples questions sur l'action des forces armées et la nécessaire discrétion sur les théâtres d'opération. En effet, les années à venir vont voir la multiplication des objets personnels connectés, comme les montres, les bracelets et autres appareils. La multiplication de ces appareils mobiles, l'usage de plus en plus courant des réseaux sociaux et de la facilité avec laquelle on peut trouver des moyens de connexion sur les théâtres d'opération, peuvent constituer un danger pour la sécurité des opérations. Par exemple, les métadonnées intégrées dans les vidéos et les photos[3] permettent la géolocalisation volontaire ou involontaire[4] des informations transmises ou publiées, informations souvent sensibles.

En outre, un certain nombre d'exemples ont pu montrer la difficulté que certains avaient maintenant à différentier la sphère privée et la sphère professionnelle. Si ce phénomène touche d'autres métiers, les conséquences potentielles sont accentuées dans les forces armées. C'est ainsi qu'en 2010 un soldat israélien a révélé l'heure et le lieu d'un raid dans une

[2] http://www.telegraph.co.uk/news/uknews/defence/10948490/Troops-leaked-confidential-data-on-Twitter-and-Facebook.html
[3] http://security.duke.edu/what-your-smartphone-photos-know-about-you
[4] http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/Lettre_IP_N-8-Mobilitics.pdf

mise à jour de son statut Facebook avec pour conséquence l'annulation de l'opération par l'armée israélienne[5]. Face à ces nouveaux usages et la généralisation de ces outils dans la vie quotidienne et professionnelle, le Ministère de la Défense français a déjà publié un guide du bon usage des médias sociaux[6] afin de sensibiliser les effectifs aux risques potentiels mais aussi en fournissant des règles pour un usage plus sécurisé. Mais la multiplicité des types d'appareils, le fait qu'ils émettent de plus en plus de manière automatique et peuvent – sans intention de leur porteur - transmettre des informations, oblige à un suivi attentif de ces évolutions technologiques. L'attention du commandement devra donc se concentrer sur les risques liés aux usages personnels, tout particulièrement quant à l'utilisation des nouveaux terminaux personnels mobiles sur les théâtres d'opérations.

Mais les réseaux sociaux n'affectent pas que la vie personnelle et la sécurité des troupes. Ils peuvent également perturber la communication des Armées et le déroulement des opérations en exposant, en dehors de toute contextualisation éditoriale, des images violentes, voire choquantes, qui peuvent atteindre les opinions publiques. Cet effet de « loupe médiatique » peut d'ailleurs transformer une action individuelle en véritable « buzz » géostratégique. Ainsi, quand en 2003 dans Bagdad «libérée», un caporal du

[5] http://www.haaretz.com/news/idf-calls-off-west-bank-raid-due-to-facebook-leak-1.264065
[6] http://www.defense.gouv.fr/guide-medias-sociaux/telecharger.pdf

4ème Régiment des Marines[7] affuble la statue de Saddam Hussein d'une bannière étoilée, l'image fait le tour du monde. Relayée par la presse, elle a eu, déjà à l'époque, des conséquences importantes pour l'Armée américaine en termes d'image. Mais on peut sans peine imaginer que 10 ans plus tard, cette image aurait certainement été relayée par et sur les médias sociaux et se serait révélée probablement un facteur d'agitation dans un certain nombre de pays.

Cette problématique va en s'amplifiant en raison notamment des performances accrues des réseaux qui favorisent, par exemple, la diffusion instantanée de vidéos. Les conséquences peuvent être nombreuses et de nature à bouleverser l'opinion publique et la conduite des missions des Armées : impact sur le moral des troupes, troubles sociaux, manipulation de l'opinion.

[7] http://www.penseemiliterre.fr/la-tentation-du-caporalisme-strategique_2013947.html

Numérisation et robotisation

Les capteurs de plus en plus intelligents et connectés présentent une formidable opportunité d'améliorer la fonction ISR[8], de réduire la boucle OODA[9], ainsi que de faciliter la gestion d'une grande flotte de systèmes et véhicules autonomes. L'utilisation des drones par les forces armées n'est pas nouvelle mais leur emploi est de plus en plus important. Ces drones permettent de franchir de manière discrète les frontières pour faire du renseignement en zone de crise et sont même utilisés par certains pays pour conduire à des éliminations physiques sur un territoire étranger. Ces nouveaux usages induisent une virtualisation de la guerre qui devient de plus en plus une « guerre à distance ».

L'utilisation de drones aériens démontre également un besoin en technicité accrue de la part du personnel des forces armées. Le recrutement devrait s'en trouver modifié avec la recherche de profils davantage technologiques d'une part et le recours plus poussé à des acteurs privés d'autre part, comme c'est le cas avec les contractants de General Atomics et de L3C pour la mise en œuvre des drones Reaper de l'Armée de l'Air française. Illustration de ces nouveaux enjeux de recrutement et de formation, celle ci se trouve d'ailleurs confrontée à un manque d'effectifs en équipage pour utiliser

[8] Intelligence, Surveillance and Reconnaissance
[9] Observer, Orienter, Décider, Agir

ses drones Reaper et a dû faire appel à l'US Air Force pour former d'avantage d'équipages au cours des temps à venir[10].

Si le recours de plus en plus systématisé aux drones aériens apporte beaucoup à la conduite des opérations, il soulève également de nombreuses questions qui ne sont pas que d'ordres moral, éthique et politique. Cette guerre « téléguidée » a aussi des conséquences notables sur les pilotes. Dans le cas de l'utilisation de drones en Afghanistan, les opérateurs sont basés dans la base de l'US Air Force à Cannon au Nouveau-Mexique. Ainsi, en appuyant sur un bouton aux États-Unis un tir de missile peut-être lancé en Afghanistan, et le soir même le tireur être revenu à la vie familiale, sans sas de décompression. Les études réalisées tendent à démontrer que ces personnes souffrent de plus en plus de stress post-traumatique lié à une trop grande proximité entre la vie réelle et la réalité de la guerre qui les conduit à une forme de dissonance cognitive[11]. Au plan psychologique, les pilotes semblent donc confrontés à de nouvelles formes de tensions liées notamment à la difficulté de *"jongler simultanément entre les exigences de la vie domestique et les phases de combat*"[12].

Sur le plan de l'efficacité des frappes menées, même si les chiffres réels de l'usage des drones armés restent

[10] http://www.opex360.com/2015/06/11/larmee-de-lair-manque-dequipages-pour-utiliser-ses-drones-male/
[11] http://www.stripes.com/mccaskill-drone-pilot-stress-is-unprecedented-1.354681
[12] http://www.lemonde.fr/ameriques/article/2013/06/18/les-blessures-a-l-ame-des-tueurs-a-distance_3432239_3222.html

confidentiels, des études ont mis en exergue que cette utilisation massive au lieu de servir au ralliement des « cœurs et des esprits » contribuerait au contraire à radicaliser les populations locales en présentant une menace permanente pour les civils qui peuvent être des victimes collatérales[13].

Enfin, le recours de plus en plus fréquent à des objets autonomes ou commandés à distance pourrait contribuer à abaisser la capacité de prise de risque chez les décideurs, ne serait-ce que pour des raisons médiatiques, rendant l'intervention humaine sur le terrain plus exceptionnelle.

Mais au delà de ces usages connus et en croissance exponentielle, l'accélération et la systématisation du recours à ces nouvelles technologies de robotisation ont le potentiel de profondément affecter l'organisation des forces armées[14]. Ainsi, une grande part des activités opérationnelles - logistique, recherche et sauvetage[15], voire jusqu'à des missions de patrouilles armées[16] - pourrait dans un futur proche être conduite à distance voire entièrement automatisée. Au croisement du numérique, de l'électronique et de la mécanique, les applications robotiques commencent

[13] http://www.cicde.defense.gouv.fr/IMG/pdf/20150127_np_cicde_fiche-implications-sociales-drones.pdf
[14] http://www.lefigaro.fr/vox/economie/2014/10/27/31007-20141027ARTFIG00330-pourquoi-la-robotisation-peut-faire-disparaitre-pres-de-la-moitie-des-emplois-d-ici-2035.php
[15] http://opexnews.over-blog.com/2014/04/us-navy-des-robots-pompiers-pour-lutter-contre-les-feux-de-navires.html
[16] http://www.opex360.com/2014/10/08/la-marine-americaine-mis-au-point-des-patrouilleurs-robotises-armes

à émerger non seulement dans la vie quotidienne [17] mais aussi dans le domaine militaire. Les applications robotiques devraient donc suivre la même tendance que celle des véhicules assistés voire autonomes : de plus en plus intelligents et autonomes et dotés de capteurs de plus en plus performants.

Cette tendance est illustrée par exemple, dans le cadre du soutien au combattant, par le robot *Big Dog*. Il a été développé par la société *Boston Dynamics* pour remplir des fonctions de support logistique pour l'Armée américaine. *Big Dog* peut ainsi accompagner les soldats sur les théâtres d'opération à une vitesse de 6km/h et porter un barda de 150kg[18] et ce sur des terrains montagneux et enneigés. Dans le soutien logistique, *L'US Army* a également récemment testé un convoi logistique formé par des camions sans conducteurs. L'idée de ce projet AMAS est d'éviter d'exposer la vie des conducteurs à la menace des engins explosifs improvisés, des embuscades ou des conditions climatiques très difficiles[19]. Autre exemple, le robot *PackBot* de la société *iRobot* est un robot de reconnaissance et de déminage qui peut effectuer des opérations de détection CBRN et manipuler des matières dangereuses. Il relaie des données

[17] http://www.lesechos.fr/18/03/2014/lesechos.fr/0203377290898_pierre-yves-oudeyer--inria------les-robots-vont-avoir-des-impacts-societaux-enormes--.htm
[18] https://www.youtube.com/watch?gl=BE&v=W1czBcnX1Ww
[19] http://www.opex360.com/2014/02/06/lus-army-a-teste-avec-succes-un-convoi-logistique-automatise/

vidéo et audio en temps réel à l'opérateur qui peut rester à une distance sécuritaire[20].

Numérisation et rattrapage technologique

Face à la multiplication des capteurs connectés, les dispositifs intelligents comme leur exploitation seront à la portée de plus en plus de personnes et d'organisations. Certaines de ces technologies se sont en effet considérablement développées dans le secteur civil. C'est le cas par exemple des drones[21] ou encore de l'imagerie satellite[22] qui sont devenus des composants essentiels de la préparation et de l'exécution de la manœuvre. Or, ces dernières années, ces deux technologies sont devenues facilement accessibles et représentent des marchés de plus en plus conséquents.

Les véhicules autonomes et les drones en sont d'excellents exemples d'actualité et démontrent que, d'ores et déjà, les capacités des drones de loisir ou des drones à but professionnel sont accessibles à tous sans contrôle et à des prix « grand public ». Certains drones du commerce disposent

[20] http://www.45enord.ca/2014/09/forces-canadiennes-20-nouveaux-robots-pour-detecter-les-agents-chimiques-radioactifs-ou-bacteriologiques/
[21] http://www.presse-citron.net/la-revolution-des-drones-en-chiffres-infographie/
[22] http://www.prnewswire.com/news-releases/commercial-satellite-imaging-market-to-reach-usd-50186-million-by-2019-globally-transparency-market-research-241139781.html

ainsi de capteurs avancés et de spécifications techniques pouvant se rapprocher de celles d'appareils mis en œuvre par les Armées, pour des prix évoluant antre 500 et 2.000 euros. De même, des images satellites avec des résolutions à 50 cm sont disponibles sur le marché, sans même parler des outils « grands publics » qui malgré leurs limitations donnent tout de même des capacités très avancées à des utilisateurs sachant les mettre en œuvre. Ces types d'appareil sont d'un maniement somme toute simple même s'il requiert un entrainement minimal et certaines compétences techniques pour sa mise en œuvre et son exploitation. Ils pourraient préfigurer de quelles manières les moyens de surveillance pourraient être mis en œuvre par des groupes adverses de faible niveau technologique. Il est même possible de les imaginer utilisés comme moyens d'action, piégés ou capables d'emporter de petites charges de quelques centaines de grammes.

Cette porosité entre les technologies civiles et militaires pourrait conduire à un rattrapage par des forces adverses, même asymétriques, dans des domaines où la supériorité des forces armées conventionnelles était jusqu'à présent incontestée. Ainsi, en 2014, Chuck Hagel, Secrétaire d'État à la Défense soulignait « *la sophistication, la technologie, l'argent, les ressources* » à disposition de Daech qui, de son côté, a largement communiqué sur ses capacités à mettre en

œuvre des drones, issus du commerce, pour préparer ses opérations[23].

Numérisation et Cybersécurité

Cet usage de plus en plus généralisé des technologies numériques soulèvent également des questions de sécurité[24] : sécurité des données d'une part, et sécurité des réseaux d'autre part. Le cyber espace présente un intérêt certain pour les organes de renseignement, dont le renseignement militaire : il est un lieu de collecte d'informations, dont le volume explose avec la croissance exponentielles des outils numériques[25].

Le monde du « tout connecté » offre une opportunité de s'introduire dans les réseaux et de les détourner. Par exemple, le moteur de recherche *Shodan* permet de trouver les objets connectés. Des journalistes norvégiens enquêtant sur cette technologie ont réussi à accéder à une plateforme d'aiguillage des trains[26] car elle n'était pas protégée. Une telle situation peut également être envisagée pour les applications militaires avec des conséquences dangereuses. Récemment, des missiles allemands de type *Patriot* déployés en Turquie

[23] http://edition.cnn.com/2014/08/24/opinion/bergen-schneider-drones-isis
[24] http://www.cnetfrance.fr/news/securite-de-l-internet-des-objets-a-l-internet-des-vulnerabilites-39796755.htm
[25] http://www.institutmontaigne.org/res/files/publications/Etude%20renseignement%20juillet%202014.pdf
[26] http://www.cil.cnrs.fr/CIL/spip.php?article2591

auraient ainsi été piratés et sous contrôle de hackers inconnus pendant un court laps de temps[27].

A l'inverse, la généralisation du chiffrement des flux transitant dans le cyberespace et des données stockées va rendre de plus en plus difficiles les interceptions et les réquisitions sur le plan technique par les agences de renseignement militaire pour tout ce qui concerne le « Renseignement d'Intérêt Militaire » (RIM). En effet, les services fournis depuis des serveurs situés à l'étranger, notamment à travers les services de *Cloud*, n'ont pas d'obligation légale de fournir les données confidentielles de leurs utilisateurs. Ces éléments peuvent être exigés directement auprès de l'utilisateur (clé de chiffrement, identifiant/mot de passe), qui peut refuser empêchant ainsi les surveillances discrètes.

Par ailleurs, la mutation à venir dans le domaine de la téléphonie (nouveaux protocoles, délocalisation des serveurs de contrôle à l'étranger, chiffrement de bout en bout des communications, perte de maitrise des opérateurs historiques) avec des technologies telles que WebRTC[28] risque de rendre inopérants les processus et les systèmes d'interceptions légales actuellement mis en place. De plus, les réseaux privés d'échanges comme TOR[29], base de

[27] http://www.welt.de/wirtschaft/webwelt/article143677997/Steuerten-Hacker-Raketenstationen-der-Bundeswehr.html
[28] Web Real-Time Communication, littéralement *communication web en temps réel*
[29] Tor (acronyme de *The Onion Router*, littéralement « le routeur oignon »)

l'Internet clandestin (« Darknet ») et se révèlent extrêmement difficiles à surveiller, même pour la NSA[30].
Le ministère de la Défense français a toutefois déjà élaboré un programme, dans le cadre de son Pacte Cyber, pour accélérer son adaptation aux menaces du cyberespace. Une enveloppe de 1 milliard d'euros est prévue pour les 5 prochaines années tandis que 500 experts devraient rejoindre l'État-major des Armées et la Direction Générale de l'Armement. Les axes de recherche concernent l'élaboration de sondes souveraines capables de surveiller les réseaux, l'architecture des systèmes, les capacités techniques de réaction à une attaque[31].

Si les nouvelles technologies numériques présentent de formidables opportunités, elles constituent dans le même temps de nouveaux défis et induisent des changements majeurs à venir pour les forces armées en termes non seulement fonctionnels mais aussi organisationnels. Les nouveaux usages du numérique contribuent à modifier les modes de fonctionnement, les conditions et le cadre d'engagement des forces armées, mais aussi la vie quotidienne des militaires. A ce titre, les ressources humaines sont un enjeu structurant pour les Armées. Si une conséquence de l'accélération des technologies de l'information est un besoin plus fort en profils techniques,

[30] http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
[h] http://www.lemonde.fr/politique/article/2014/02/06/1-milliard-d-euros-pour-faire-face-a-la-cyberguerre_4361846_823448.html

l'autre est celle de la formation et de l'entrainement des militaires.

En effet, les systèmes d'armes devenant de plus en plus complexes et sophistiqués, les formations et l'entrainement des militaires représentent des enjeux majeurs pour les États. De par la rapidité des évolutions technologiques et de la multiplication des technologies « duales », ces enjeux n'en deviendront que plus importants. Ainsi, l'ergonomie des interfaces est déjà une problématique essentielle qui devrait prendre de plus en plus d'ampleur dans les prochaines années.

Numérisation et formation

La transformation des Armées n'est pas de nature à remettre en question la mission fondamentale de la chaîne de formation. Tout en conduisant les restructurations, il s'agit bien de poursuivre les efforts entrepris pour développer chez les jeunes cadres, une véritable identité militaire, socle des valeurs sur lesquelles se fondent compétences, esprit de discipline et exemplarité.

La formation virtualisée (simulation, réalité augmentée, etc.) n'est pas nouvelle. Des simulateurs types *First-Person Shooter* ou *Full Flight simulator* existent déjà depuis un certain nombre d'années. Cependant, l'utilisation de nouveaux outils de simulation ou de *gamification* pourrait aller en s'amplifiant. Ils présentent des avantages certains pour les forces armées. En effet, ils permettent de jouer des scénarios complexes -notamment par le biais de jeux sérieux - difficilement réalisables « en vrai » par l'ampleur des moyens matériels et humains à mettre en œuvre. Par ailleurs, la possibilité d' entrainer et de former des militaires, par équipe ou indépendamment, ensemble ou à distance, permet de rationaliser et de gagner du temps sur les cycles de formation. Toutefois, la guerre est un acte collectif et le facteur humain reste décisif pour le bon fonctionnement des Armées. Ainsi, l'attention des cadres-instructeurs de contact, l'émulation du groupe, l'exigence de performance collective,

l'esprit de promotion doivent continuer à être des instruments pédagogiques dans les formations militaires.
En effet, la formation est le processus d'acquisition de savoir-faire et de savoir-être qualifiant un individu pour tenir une fonction dans la communauté militaire. Elle comprend deux volets : l'instruction individuelle et l'éducation. Elle est à distinguer de l'instruction collective qui agrège des savoir-faire individuels au sein d'une fonction opérationnelle et de l'entraînement qui est un processus d'entretien des savoir-faire collectifs associant plusieurs fonctions pour l'exécution d'une mission donnée.

Éduquer pour savoir apprendre et réussir.

S'engager dans un apprentissage requiert une nécessaire motivation et un besoin de confiance en soi, de la part de celui qui apprend. Les enseignants ont le souci d'agir sur les leviers de la motivation mais notre culture de l'exigence nous conduit parfois à souligner les faiblesses plus qu'à encourager les efforts. C'est notamment vrai dans les situations d'interrogation sur le niveau des élèves. Si l'enseignant est persuadé que le niveau est faible, les occasions de le prouver se présenteront toujours. S'il est persuadé que le stagiaire réussira, et s'il lui communique cette confiance, il réussira au-delà même de son imagination. Ceci n'est pas démagogie et n'empêche nullement l'exigence et la rigueur dans les apprentissages; mais l'essentiel est bien de convaincre celui qui apprend qu'il y arrivera, de lui soumettre une situation à

sa mesure pour le lui prouver, et enfin de le mener progressivement vers l'objectif final.

Concilier théorie et pratique.

Les place et rôle respectifs de la théorie et de la pratique, du « réfléchir » et de l'agir », méritent un examen particulier, dans les processus d'enseignement. Théorie puis pratique : c'est souvent cet ordre que l'enseignement propose. L'éducation nationale oriente d'ailleurs souvent les élèves les plus fragiles vers l'apprentissage, vers des espaces de formation où ils doivent d'abord faire, avant de comprendre, analyser puis conceptualiser. Les plus performants accèdent pour leur part davantage à des études supérieures.

La pratique peut très bien précéder la théorie voire l'introduire. La mise en situation précoce offre certains avantages : prise de conscience du besoin d'apprendre, état des lieux des acquis, motivation et émulation, conscience de la finalité. Des connaissances peuvent ainsi être distillées progressivement jusqu'à réussir la mission. Commence alors une phase d'analyse dont la théorie devient la synthèse concrète plus facilement abordable.

Numérisation et commandement

Au plus haut niveau, les nouveaux outils numériques permettent au commandant militaire d'avoir une vue sur la totalité du théâtre d'opération. Cette capacité du chef militaire à avoir une vue sur la totalité des unités sur le terrain peut être un facteur d'efficacité opérationnelle. Mais elle pourrait aussi être ressentie comme un risque d'entrisme et de micro-management par les unités subordonnées et conduire à un écrasement des niveaux de commandement, alors que le principe de subsidiarité reste un gage de l'esprit d'initiative dans la conduite des opérations sur le terrain.

Cette « vision à 360° » du chef peut avoir des effets positifs comme une analyse avec plus de recul sur la situation. Mais l'utilisation massive d'outils de simulation et de virtualisation peut également engendrer une vision faussée, « idyllique », d'une situation et de l'état de ses acteurs. De l'écran – même et surtout ultra-réaliste - à la réalité sur le terrain, il existe un risque de prise en compte insuffisante des facteurs humains dans la conduite au contact et l'analyse de situation (fatigue, stress, conditions réelles – au sens non-virtuelles – de l'engagement). Par ailleurs, les travaux sur les jeux vidéo ont démontré que dans une certaine mesure le rapport à la réalité pouvait être modifié pour les utilisateurs engendrant

des possibilités de confusion entre la réalité et la fiction vécue à travers les jeux[32].

Une autre problématique sous-jacente est celle de la prise de décision. Par l'accroissement et l'automatisation des émetteurs et des volumes de flux d'information, il existe un risque de paralysie. Toute décision – et en tout premier celle du chef au combat – s'effectue dans un environnement dit incertain ce qui par nature engendre une prise de risque. La tentation peut être grande de rechercher une situation de connaissance « pleine et parfaite » en disposant de toutes les informations possibles avant de prendre une décision, et donc par là réduire le risque.

[32] http://www.ipubli.inserm.fr/bitstream/handle/10608/103/?sequence=13

Publications récentes

MCO des moteurs d'hélicoptères militaires - Juin 2015 - English version available

Le SIA Lab – L'innovation au service de la Défense - Juin 2015

Systèmes d'information opérationnels et de communication (SIOC) en Europe - Avril 2015 - disponible en anglais

Afghanistan, Côte d'Ivoire, Libye, Mali, Centrafrique : Perspectives de 10 ans d'engagements extérieurs - Septembre 2014

Redimensionner notre dissuasion : Quels risques ? Quels gains ? Eclairages sur un débat d'actualité - Septembre 2014

Le MCO aéronautique : un enjeu pour la cohérence capacitaire des armées - Septembre 2014 – English version available

Les atouts stratégiques de la maîtrise de la troisième dimension - Septembre 2014

Une nouvelle approche du terrorisme - Mai 2013 - English version available

CEIS

Société Anonyme au capital de 150 510 €

SIRET : 414 881 821 00022 – APE : 741 G

280 boulevard Saint Germain – 75007 Paris

Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60

ceis