

RDN

Penser demain

66^e session du Centre des hautes études militaires

Les Cahiers de la
Revue Défense Nationale



Penser demain

66^e session du Centre
des hautes études militaires (CHEM)

Sommaire

7 Introduction

FRÉDÉRIC BOUCHER

Penser la défense de l'Europe

11 La défense du territoire européen, enjeu de la décennie à venir pour la France ?

MARC-ANTOINE DE SAINT GERMAIN

Havre de paix depuis plus de 70 ans, l'Europe est désormais confrontée à des défis existentiels tant internes (*Brexit*, flux migratoires massifs, montée des populismes, fragilité de la zone euro), qu'externes avec la résurgence à sa périphérie des États-puissances (Chine, Russie) et des zones grises (Moyen-Orient, Maghreb, Balkans) au sein desquelles des Nations émergentes refusent comme la Turquie le modèle des démocraties européennes. Dans un contexte de repli des États-Unis, entamé depuis 2009 avec Barack Obama et confirmé par l'administration Trump, les Européens devront assurer par eux-mêmes la sanctuarisation de leur territoire, sous peine de voir à nouveau des conflits émerger en son sein. Plus qu'une nécessité, cet enjeu stratégique devrait leur permettre de définir à nouveau un projet commun leur permettant de dépasser leurs dissensions.

25 Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ? Quelles conséquences stratégiques pour la défense européenne ?

BERTRAND JARDIN

Le désengagement militaire américain d'Europe est une tendance de fond depuis la fin de la période de la guerre froide, traduction de l'évolution de la place de l'Europe dans la stratégie globale américaine dont le nécessaire rééquilibrage vers la région Asie-Pacifique en est l'une des manifestations. Si les États-Unis n'entendent pas pour autant abandonner tout *leadership* sur le vieux continent, il n'en demeure pas moins que la perception que peuvent avoir les pays européens de cette stratégie, couplée à la prise de conscience des limites du parapluie américain face aux défis sécuritaires auxquels l'Europe est confrontée, peut jouer le rôle d'électrochoc d'une défense européenne maintenue artificiellement en vie.

40 Les possibles évolutions de la relation franco-britannique d'ici dix ans

ROBERT J. THOMSON

Cette étude examinera d'abord le contexte des relations franco-britanniques dans les dix années à venir et comment ce contexte international pourrait faire évoluer ces relations au niveau politico-militaire. Par la suite, les *game-changers* potentiels, qui pourraient menacer ce rapport seront examinés. Enfin, il sera proposé quelques domaines dans lesquels la France et le Royaume-Uni pourraient approfondir leur relation.

53 Vers une Union européenne de la sécurité et défense Défis et perspectives de la politique allemande et de la relation Allemagne-France

FRANK WACHTER

Dans le contexte d'un environnement sécuritaire dégradé et avec une Allemagne prête à jouer un rôle plus actif sur la scène internationale, il est grand temps de renforcer notre solidarité et les capacités européennes afin de protéger plus efficacement nos frontières et les citoyens de l'UE, et de contribuer à la paix et la stabilité dans notre voisinage. Le *Brexit* serait l'occasion stratégique de relancer le projet d'une « Union européenne de la défense et de la sécurité » en le basant sur la « Stratégie globale » récemment présentée par Federica Mogherini. Le succès de ce projet dépendra avant tout de la capacité de la France et de l'Allemagne à converger et maintenir une vision stratégique commune et partagée.

67 **Renforcement de la fonction « protection » à l'horizon 2030**

PHILIPPE DEDOBBELEER

Face à l'islamisme radical et au retour des États-puissances qui constituent une menace continue, durable et globale sur le territoire national, la Nation doit être capable d'affronter tout type d'agressions. Le principal défi va bien au-delà du renforcement des cinq postures de protection : il s'agit de construire une posture réactive et intégrée à l'échelle du pays. Il faut réussir à fédérer, avec maîtrise, les acteurs et les moyens du pays qui contribuent, directement ou non, à la fonction stratégique de défense et de sécurité « protection ». Cette montée en puissance doit naturellement se faire en respectant les garanties offertes par l'État de droit aux individus et à la société.

79 **De la conduite et de la planification des opérations intérieures**

STÉPHANE MARCHENOIR

La conduite des opérations extérieures (Opex) a démontré l'intérêt majeur que constitue le Centre de planification et de conduite des opérations (CPCO) aux ordres directs du Céma. Créé en 2003 et issu du COA (opérations des armées) – transformé en COIA (interarmées) – mis en place à partir de 1976, le CPCO a principalement permis d'améliorer la conduite des opérations grâce notamment à un meilleur dialogue avec le ministère des Affaires étrangères. Avec *Sentinelle*, la dimension intérieure s'est accrue et exige une amélioration des échanges entre les forces, les services et le ministère de l'Intérieur par une meilleure connaissance mutuelle. Une relation étroite entre la Défense et ce ministère, s'appuyant sur les acquis et l'expérience du CPCO, sera un gage d'efficacité supplémentaire pour nos opérations intérieures.

91 **Avant-postes de forces légères**

LAURENT CLUZEL

Formule prompte à la rêverie tactique, emportée par l'élan des hussards de Lasalle ou des parachutistes de Bigeard. Formule forte sur le plan opératif, si l'on imagine l'organisation induite du commandement et du soutien. Formule chargée de sens, rapportée au niveau stratégique, dans un univers dangereusement imprévisible. État d'esprit avant tout, pour veiller sur les siens, faire face et prendre l'initiative. Force morale, force vitale.

109 **Commander les opérations en 2030 : quel équilibre entre centralisation réactive et réalités de terrain ?**

THIERRY GARRETA

La numérisation des espaces de bataille, permettant de suivre en direct l'ensemble des vecteurs et systèmes de combat connectés, va-t-elle conduire à revoir l'architecture traditionnelle de la chaîne de commandement, lorsque le niveau central sera en mesure de tout voir et de tout diriger ? Si la doctrine interalliée et les réalités de terrains interarmées militent pour conserver un certain nombre de repères, un accompagnement du progrès semble inévitable. Le C2 s'impose progressivement comme système de combat et provoque des mutations dans le commandement des opérations.

122 **Quelles orientations face au déni d'accès à l'horizon 2025 ?**

BRUNO FOUSSARD

Ce travail vise à expliquer les enjeux du déni d'accès, encore mal considérés dans le monde de la défense car souvent abordés sous un angle technique et tactique. Dans ce but, il tente de démontrer que ce concept ne considère pas que le haut du spectre et la puissance aérienne, mais a des implications stratégiques sur l'ensemble de nos forces et sur nos ambitions politiques. Il propose des orientations pragmatiques, dans un horizon contraint ne permettant pas de remédier à cette problématique par des solutions programmatiques.

141 **Robots et intelligence artificielle : quelle place pour l'homme dans les futures capacités militaires françaises ?**

OLIVIER BEAURENAUT

Le militaire a le devoir d'appréhender les ruptures susceptibles de bouleverser les modalités de la guerre. L'ingénieur a quant à lui vocation à capter, comprendre et orienter les innovations technologiques en cours pour développer, en maîtrisant risques et coûts, les solutions, architectures et applications les plus pertinentes et efficaces permettant, *in fine*, de disposer des capacités et services déterminants pour de futurs rapports de forces favorables. La robotique et l'intelligence artificielle, à l'origine de la 4^e révolution industrielle qui débute, constituent un *game changer* sur l'ensemble de ces champs. La communauté de défense doit en prendre la pleine mesure et s'organiser pour en tirer le meilleur parti. Son succès reposera sur notre capacité à appréhender la transformation robotique objectivement, globalement et ensemble, comme cela a été le cas pour la dissuasion nucléaire après-guerre, en restant suffisamment ouvert et créatif.

164 **Principaux enjeux des objets connectés pour la défense, et le Verbe s'est fait chair**

FRÉDÉRIC BARBRY

Les objets connectés occupent la Une des journaux ou des matinales radiophoniques. Pour autant, ils sont présentés essentiellement au grand public sous un angle ludique, masquant de ce fait leur potentialité infinie. Toutes proportions gardées, le désintérêt relatif de la communauté militaire française pour ce segment prometteur s'avère tout aussi coupable que le refus de l'arbalète au XII^e siècle. En effet, l'accroissement de leur valeur (entendre efficacité opérationnelle) apportée tient plus par le resserrement de la maille qu'ils tissent que par l'exploitation des données brutes qui en sont issues. À terme, avec les capacités de *post*-traitement autorisées par le *big data*, c'est tout l'art de la guerre qui va se métamorphoser. Demain, avec l'apparition des systèmes prédictifs, c'est toute une nouvelle philosophie du commandant qu'il convient d'anticiper.

176 **Le cyberspace, nouvel espace de souveraineté à conquérir**

CHRISTOPHE GASANÇON

Le cyberspace est un milieu matériel, immatériel et transverse aux autres milieux. *Internet* en est la première matérialisation où s'exercent des conflictualités qui lui sont propres, favorisant l'attaque par rapport à la défense. Deux visions s'y opposent. L'une techniciste voit le cyberspace comme un milieu universel, libre et sans frontières, vecteur d'une nouvelle prospérité économique. L'autre y voit un milieu identique aux autres dans lequel chaque État doit pouvoir exprimer sa souveraineté et pas uniquement en termes de défense et de sécurité, mais aussi par un cadre et des réponses aux enjeux socio-économiques de l'espace informationnel. La mise en place d'une gouvernance internationale et d'un « Montego Bay » du cyberspace constitue le cadre préalable à la reconnaissance de cette souveraineté, où la donnée en est le cœur en tant que ressource stratégique du pays d'où elle émane. Dans cet affrontement géopolitique, la France n'a pas d'alternative que de se faire entendre et développer son modèle de souveraineté numérique. Un Commissariat à l'espace numérique et aux nouvelles technologies serait le chef d'orchestre de cette partition nationale.

192 **Révolution numérique : vers une armée numérique ?**

ERWAN ROLLAND

L'organisation actuelle de notre outil de défense ne doit pas être un frein aux potentialités que laissent entrevoir la révolution numérique, les technologies émergentes et les ruptures qu'elles préfigurent. La croissance rapide des technologies de l'information et de la communication, et l'innovation dans les systèmes numériques nécessitent de se poser la question sur la pertinence de bâtir dès à présent un modèle d'armée numérique capable de répondre aux défis à venir. Sur la base d'un état probable de maturité de ces nouvelles technologies et des menaces qu'elles font déjà peser sur nous, cette étude se propose de jeter les contours que pourrait prendre une véritable armée numérique. L'enjeu pour la France et ses armées est de disposer d'une organisation dédiée lui permettant d'assurer sa défense et sa sécurité en optimisant l'emploi et les potentialités numériques du cyberspace, en parfaite complémentarité avec les forces conventionnelles des autres milieux.

207 **La loi d'Augustine est-elle une fatalité pour les armées françaises à 10 ans ?**

DAMIEN WALLAERT

Si elle est indispensable à la conservation d'une supériorité sur l'ennemi, la technologie sera toujours en concurrence avec le nombre. Mais la loi d'Augustine n'est pas une fatalité pour les armées françaises. Il apparaît en effet inéluctable et possible d'établir, voire de rétablir, un équilibre entre la nécessité de conserver l'ascendant technologique sur l'adversaire et celle de garder une autre source essentielle de puissance : un volume de forces suffisant.

221 **Les prestations de soutien commun du SCA à horizon 2020-2025 : évolutions comportementales des bénéficiaires et réponses à apporter**

ANNE TÊTE

Les armées françaises vont accueillir dans les prochaines années les jeunes des générations Y et Z, qui ont été nourries au lait de la technologie et dont les attentes et la relation au travail sont très différentes de celles de leurs parents. Les forces armées devraient rester attractives par leurs missions mais elles ne pourront faire l'économie d'une modernisation du soutien quotidien du militaire, sous peine de manquer leur rendez-vous avec ces jeunes générations. Le numérique, le *big data*, les objets connectés, mais aussi les évolutions réglementaires et de procédures doivent sous tendre la réflexion qui est à conduire à marche rapide dans une démarche collective et partagée.

236 **Associations professionnelles nationales de militaires et dialogue social dans les forces armées**

FRÉDÉRIC BOUDIER

En l'absence de représentation syndicale dans les armées, le ministère de la Défense a progressivement mis en place au cours des dernières décennies un dispositif de concertation reposant à l'échelon central sur le Conseil supérieur de la fonction militaire (CSFM) puis, au sein des principales forces armées ou formations rattachées, sur des Conseils de la fonction militaire (CFM). Ces instances nationales ont été prolongées à des degrés divers au sein de chaque force par des instances de représentation locale. La loi du 28 juillet 2015, instaurant des Associations professionnelles nationales de militaires (APNM) qui ont vocation à traiter des questions relatives à la condition militaire, notion définie d'ailleurs dans cette même loi, vient modifier et compléter ce dispositif de concertation. Ces associations devront cependant trouver leur juste place dans les prochaines années au sein d'un dispositif de concertation déjà installé.

251 **Le Pentagone Citoyen, plaidoyer pour une mobilisation nationale face à un ennemi insaisissable**

CYRIL CARCY

Les attentats dramatiques, qui ont endeuillé la France depuis 2015, font progressivement émerger l'esprit de défense dans la pensée nationale. Les articles fleurissent, encourageant la société française à plus de vigilance face à un ennemi aussi imprévisible qu'invisible. Avec cette accélération inéluctable des opérations djihadistes au cœur d'une société anomique, cette prise de conscience apparaît clairement insuffisante. Avant qu'elle ne mue en une forme ombrageuse, guidée par une soif de représailles, cette mobilisation mériterait d'être portée par une volonté politique et d'être déclinée au travers d'une approche globale. Le *Pentagone Citoyen* consisterait à associer les acteurs cardinaux de la vie de la cité pour faire émerger un *modus vivendi* réinventé qui s'appuierait utilement sur les armées comme parangon sociétal. L'avènement d'un tel état d'esprit présente un double bénéfice : celui d'entraver l'action terroriste tout en confortant la résistance de la société française face aux chocs et aux surprises stratégiques à venir.

La *Revue Défense Nationale* est éditée par le Comité d'études de défense nationale
(association loi de 1901)

Adresse géographique : École militaire, 1 place Joffre, Paris VII

Adresse postale : BP 8607, 75325 Paris cedex 07

Fax : 01 44 42 31 89 - www.defnat.fr - redac@defnat.com

Directeur de la publication : Alain Coldefy - Tél. : 01 44 42 31 92

Rédacteur en chef : Jérôme Pellistrandi - Tél. : 01 44 42 31 90

Rédactrice en chef adjointe : Audrey Hérisson

Secrétaire général et *webmaster* : Paul Laporte - Tél. : 01 44 42 31 91

Secrétaire général de rédaction : Pascal Lecardonnel - Tél. : 01 44 42 43 69

Assistante de direction et secrétaire de rédaction : Marie-Hélène Mounet - Tél. : 01 44 42 43 74

Secrétaire de rédaction : Jérôme Dollé - Tél. : 01 44 42 43 69

Abonnements : Éliane Lecardonnel - Tél. : 01 44 42 38 23

Chargés d'études : Laurent Henninger et Emmanuel Desclèves - Tél. : 01 44 42 43 72

Régie publicitaire (ECPAD) : Karim Belguedour - Tél. : 01 49 60 58 56

DL 92068 - 4^e trimestre 2017 - ISSN : 2105-7508 - CP n° 1019 G 85493 du 4 décembre 2014

Imprimée par Bialec, 23 Allée des Grands Pâquis, 54180 Heillecourt

Introduction

« Le présent accouche, dit-on, de l'avenir. »

VOLTAIRE (1694-1778)

« L'avenir ne sera pas ce qui va arriver, mais ce que nous allons faire. »

Henri BERGSON (1859-1941)

Le Centre des hautes études militaires (CHEM) a été créé en 1911 à l'initiative du général de brigade Ferdinand Foch. Il est interarmées depuis 1952 et multinational depuis 2000. Il prépare chaque année trente auditeurs français et étrangers, du grade de colonel, capitaine de vaisseau ou équivalent, aux hautes responsabilités qui leur seront confiées dès leur sortie du CHEM, en consolidant leurs qualités personnelles de chef et de cadre dirigeant, en complétant leurs connaissances du fonctionnement de l'État, du ministère et de l'environnement de la défense, des relations internationales et en développant leur compréhension de la relation politico-militaire.

Les meilleurs d'entre eux ont vocation à armer dans dix ans les postes sommitaux de la hiérarchie militaire. Cette année de réflexion et d'étude au CHEM a été l'occasion de se projeter à cet horizon. Invité à « Penser demain », chacun a ainsi réalisé une étude prospective, dont quelques-unes sont proposées à votre lecture dans ce *Cahier de la Revue Défense Nationale*.

* * * * *

La période 2016-2017 a été marquée par des évolutions majeures, certaines prévisibles, d'autres plus surprenantes, qui ont bousculé les équilibres de l'ordre mondial et rendu l'avenir encore plus incertain : lutte contre *Daesh* et un terrorisme d'inspiration islamiste qui frappe au cœur même des démocraties occidentales, crise migratoire sans précédent, dérive autoritaire de certains dirigeants européens, démonstration de force des « États-puissance », conséquences du Brexit et de l'élection d'un nouveau Président aux États-Unis...

Dans ce contexte bouleversé, alors même que la campagne pour l'élection présidentielle battait son plein en France, les auditeurs de la 66^e session du CHEM réfléchissaient sur un certain nombre de thématiques intéressant la Défense en se projetant dans l'avenir, exercice toujours délicat...

Compte tenu du nouveau contexte géostratégique, il apparaît clairement que la défense du territoire, considérée sous un angle européen, s'impose comme un enjeu de la décennie pour la France (CV **Marc-Antoine DE SAINT GERMAIN**). Le relatif désengagement américain d'Europe, entre trompe l'œil et réalité, pose la question des conséquences stratégiques pour la défense européenne (Col. (A) **Bertrand JARDIN**). Les regards britannique (GBR **Robert J. THOMSON**) et allemand (Col. (*Heer*) **Frank WACHTER**) confortent la nécessaire prise de conscience des grands pays d'Europe de l'impérieuse nécessité de mieux prendre en charge leur défense et de maintenir, voire de consolider, leurs partenariats stratégiques.

* * *

Ce cadre posé, plusieurs pistes d'investigation se dessinent, touchant aux missions même des armées, à leur transformation, à leur adaptation aux évolutions technologiques. C'est le défi du renforcement de la fonction stratégique « Protection », pour répondre à l'attente première des Français de sécurité sur le territoire national en termes de missions et de capacités (Col. (A) **Philippe DEDOBBELEER**), ainsi que de commandement (Col. (T) **Stéphane MARCHENOIR**), mais également de posture préventive adaptée et d'agilité des forces (Col. (T) **Laurent CLUZEL**). Dans le domaine de l'intervention extérieure se pose la question du commandement des opérations dans le futur et de l'équilibre entre une centralisation réactive et les réalités du terrain (Col. (A) **Thierry GARRETA**), dans un contexte où le développement des moyens de déni d'accès remet en question notre capacité d'entrée en premier (Col. (A) **Bruno FOUSSARD**).

* * *

Ces réflexions ne sauraient être dé-corrélées d'une étude des conséquences pour les armées des évolutions technologiques extrêmement rapides :

- en termes de place de l'homme dans les futures capacités militaires françaises alors que se dessinent la banalisation de la robotisation et de l'intelligence artificielle (ICA **Olivier BEAURENAUT**) ;
- en termes d'enjeux à venir du développement des objets connectés (Col. (T) **Frédéric BARBRY**) ;
- en termes de cyberspace, nouvel espace de souveraineté numérique à conquérir (Col. (T) **Christophe GASANÇON**) ;
- plus généralement, en termes d'adaptation des armées à l'univers numérique (Col. (T) **Erwan ROLLAND**).

* * *

Parmi d'autres, quelques conditions encadrantes se dessinent, susceptibles de favoriser, ou *a contrario* de freiner, l'adaptation des armées et plus généralement de la Défense aux enjeux du futur :

- la réponse aux défis des coûts croissants des équipements, ou comment éviter la fatalité de la loi d'Augustine (Col. (T) **Damien WALLAERT**) ;
- la réponse aux attentes légitimes de soutien de la vie quotidienne des hommes et femmes des armées par les services interarmées, et singulièrement le commissariat des armées (CRCI **Anne TÊTE**) ;
- en corollaire, les évolutions possibles du « dialogue social dans les forces armées » (Col. (G) **Frédéric BOUDIER**).

* * * * *

Plus encore, et c'est à la fois une condition et la conclusion, c'est bien la volonté de se défendre du pays et de ses citoyens qui fonde tous ces enjeux, « Pentagone citoyen » permettant une vraie mobilisation dans ce contexte particulièrement difficile (Col. (A) **Cyril CARCY**).

GBR Frédéric BOUCHER
Directeur du CHEM



■ **Penser la défense de l'Europe**

RDN

Les Cahiers de la Revue Défense Nationale

La défense du territoire européen, enjeu de la décennie à venir pour la France ?

Marc-Antoine DE SAINT GERMAIN

| Capitaine de vaisseau, auditeur de la 66^e session du Chem.

Havre de paix depuis plus de 70 ans, l'Europe est désormais confrontée à des défis existentiels tant internes (*Brexit*, flux migratoires massifs, montée des populismes, fragilité de la zone euro) qu'externes (résurgence à sa périphérie d'États-puissances, zones grises) sans oublier le terrorisme qui met à mal le modèle démocratique européen. Dans un contexte de repli des États-Unis, entamé dès 2009 par Barack Obama et confirmé par l'administration Trump, les Européens devront dans la décennie à venir assurer par eux-mêmes la sanctuarisation de leur territoire, sous peine de voir à nouveau des conflits émerger en son sein.

Plus qu'une nécessité, cet enjeu stratégique devrait leur permettre de redéfinir un projet commun leur permettant de dépasser leurs dissensions. Pour cela, la France devra déterminer une nouvelle approche dans sa stratégie militaire, en coopérant de façon plus intense avec ses principaux alliés européens pour développer une capacité de démonstration de puissance, fondée sur sa dissuasion nucléaire désormais unique au sein de l'Union européenne.

Une Europe de plus en plus fragilisée en interne

Une lente désagrégation

Dans un état de grande fragilité, l'Union européenne est à un moment critique de son existence. L'essoufflement de sa dynamique date sans doute de 2005, année des négociations d'une constitution européenne sous l'impulsion de la France, et rejetée aussitôt par un vote des Français...

Une déconstruction lente se fait donc sentir depuis une douzaine d'années, conséquence du déni de confiance des peuples eux-mêmes vis-à-vis des institutions européennes et des dirigeants de leur propre pays face aux injonctions de ces derniers pour toujours « plus d'Europe », ou leurs discours moralisateurs appelant à dépasser les égoïsmes nationaux : « un fossé entre élites européistes et populations s'est ainsi creusé au fil des années. Il est devenu le problème numéro un. Le plus dangereux » ⁽¹⁾.

(1) H. VÉDRINE, *Sauver l'Europe*, p. 12.

La défense du territoire européen,
enjeu de la décennie à venir pour la France ?

Le monde rêvé par l'Europe a vécu et les contradictions entre Européens sont mises à jour après avoir été trop longtemps escamotées. Au premier plan, l'élargissement effréné de l'Union européenne, comme dette morale à la suite des conflits mondiaux, est une des causes majeures de ce rejet. Ensuite, la volonté des institutions européennes de se mêler de tout et de régenter dans le détail la vie des citoyens a engendré chez ces derniers un sentiment de perte de liberté et d'identité.

Ce rejet long et insidieux, masqué par les institutions elles-mêmes, a abouti au vote des Britanniques le 23 juin 2017 en faveur d'une sortie du Royaume-Uni de l'Union. « L'Union européenne est donc un organisme affaibli, miné de l'intérieur. (...) Elle rassemble des États-membres qui fonctionnent sur la base de la démocratie représentative, laquelle est de plus en plus contestée partout dans le monde par une revendication croissante et vengeresse de démocratie participative ou même directe » ⁽²⁾.

Devenu un vaste espace sans frontières claires, culturellement uni mais politiquement divisé, sa recherche d'identité originelle et non assouvie révèle une bataille des idées entre un projet fondé sur une communauté de valeurs cherchant à dépasser les rivalités des nations et celui d'une puissance européenne replaçant les cultures et religions au centre de la construction. Sans jamais avoir résolu cette difficulté, les Européens ont cru que la démocratie se diffuserait par simple contact et qu'un agrégat de partis démocratiques créerait un ensemble démocratique.

Il nous faut espérer que l'arrivée d'une nouvelle administration américaine plaçant sa politique intérieure au centre de ses préoccupations finira par réveiller l'UE de sa torpeur. Car elle n'a cessé de décevoir ses citoyens : « En mars 2000, le sommet européen avait fixé un objectif stratégique pour l'Union : devenir l'économie de la connaissance la plus compétitive du monde en l'espace d'une décennie. Cette stratégie de Lisbonne n'a pas été appliquée, et la distance s'est accrue entre la réalité européenne et le modèle californien » ⁽³⁾.

Aujourd'hui, l'Europe est un empire fragile et décentralisé qui cherche à résoudre ses difficultés internes par une fuite en avant administrative face à des peuples inquiets et sceptiques, sans réussir pour autant à résoudre ses différends politiques. Le Sommet de l'UE à La Valette (Malte) le 3 février 2017 a mis à jour la mécanique d'une possible autodestruction des institutions européennes, attisée par les positions dures du Président américain récemment élu contre les usages transatlantiques, les règles internationales ou le libre-échange, et au moment où le Brexit devient une réalité au Parlement britannique : « ce qui se joue, c'est l'avenir même de l'Union » ⁽⁴⁾. Il faut remonter à 2003, dans une période toutefois très différente pour la construction européenne (l'Allemagne et la France avaient alors un projet politique commun), pour observer des fractures aussi importantes en Europe. Alors divisée sur l'intervention en Irak, les États-Unis étaient déjà un facteur de fragilisation. La perspective actuelle d'un éventuel rapprochement entre les États-Unis et la Russie tétanise les pays de l'Europe

(2) H. VÉDRINE, *Sauver l'Europe*, p. 23

(3) R. GIRARD, « Le cadeau de Trump à l'Union européenne », *Le Figaro*, 30 janvier 2017.

(4) F. HOLLANDE, Sommet des chefs d'État et de gouvernement de l'UE, 3 février 2017.

de l'Est et les États baltes quand le Royaume-Uni cherche à rétablir sa « *special relationship* » avec son grand neveu américain. Pourtant, « la désintégration de l'UE ne conduirait pas à la restauration de souverainetés nationales chimériques, (...) mais au contraire à une dépendance accrue au profit des superpuissances que sont les États-Unis, la Russie et la Chine » ⁽⁵⁾.

Vers la fin d'un modèle ?

Initiatrice et facteur de paix dans le monde jusqu'à présent, l'Europe se pose la question de la pérennité de son modèle. Ne pesant plus par ses valeurs, par ses normes ou par la force de sa société civile, elle n'est plus un exemple à suivre pour beaucoup de nations émergentes. Bien au contraire, le modèle qui semble désormais s'imposer est celui d'États-puissances ayant fortement investi dans les domaines régaliens. Au risque de faire renoncer à leur population une partie de leurs libertés individuelles, seul moyen efficace semble-t-il identifié par leurs dirigeants pour traiter la question du multiculturalisme qui caractérise désormais la plupart de ces pays.

La construction européenne fondée sur l'idée *post*-guerre d'une disparition en son sein des rapports de force rend aujourd'hui son existence très fragile. L'Europe fait désormais le vide autour d'elle et participe, en partie, à la déstabilisation de son environnement immédiat. N'ayant pas su développer une politique étrangère cohérente, elle s'est bornée à une « politique de voisinage » ⁽⁶⁾.

Publié il y a vingt ans, *Le choc des civilisations* de Samuel Huntington a été très critiqué parce qu'il avait une approche un peu trop simplificatrice pour expliquer les problèmes conflictuels que rencontre la planète. Pourtant son analyse fondée sur l'existence selon lui de huit civilisations – dont les rapports entre elles seraient caractérisés par leurs affinités ou au contraire leurs différences culturelles – reste pertinente dans le contexte international actuel. Considérant que « les principes philosophiques, les valeurs fondamentales, les relations sociales, les coutumes et la façon de voir la vie en général diffèrent sensiblement d'une civilisation à l'autre » ⁽⁷⁾, la question du déclin de la puissance occidentale se pose. Pire, si certaines civilisations tentent encore d'imiter l'Occident, et l'Europe en particulier, d'autres au contraire cherchent à lui résister, particulièrement celles de tendance confucéenne ou musulmane.

La mondialisation a érodé le paysage postcolonial, qui a été jusqu'à présent composé d'États-Nations théoriquement égaux, à l'image d'une Europe apaisée : elle « a creusé les roches friables des États faibles jusqu'à la roche mère des structures traditionnelles » ⁽⁸⁾. Aux côtés desquels des empires ont réorganisé les affiliations politiques et les appartenances collectives : selon Bayram BALCI (chercheur au Ceri), « c'est la faiblesse du monde occidental, son absence de vision et de politique claire, qui poussent Ankara à se forger de nouvelles alliances » ⁽⁹⁾.

(5) D. TUSK, Sommet des chefs d'État et de gouvernement, 3 février 2017.

(6) D. DE VILLEPIN, *Mémoire de paix pour temps de guerre*, p. 523.

(7) S. HUNTINGTON, *Le choc des civilisations*, p. 137.

(8) D. DE VILLEPIN, *Mémoire de paix pour temps de guerre*, p. 94.

(9) Cité par I. LASSERRE, « La défiance s'installe entre l'Otan et Ankara », *Le Figaro*, 26 janvier 2017.

La défense du territoire européen,
enjeu de la décennie à venir pour la France ?

Une Europe économiquement fragile peu engagée militairement

Aujourd'hui, l'Europe est donc en péril, l'Allemagne ne pouvant qu'espérer des réformes courageuses en France afin que celle-ci retrouve sa souveraineté financière, préalable à la continuité de sa souveraineté sécuritaire. C'est une condition indispensable au maintien de la zone euro, dont la robustesse n'est assurée que si France et Allemagne restent en phase sur le plan économique : « Il y aura une Union européenne à différentes vitesses »⁽¹⁰⁾.

Un éclatement de la zone euro serait sans doute un cap irréversible vers la fin de l'Union européenne, nous renvoyant des décennies en arrière, avec un risque réel du retour de la guerre en Europe. Or, le budget de défense cumulé des Européens est sous la barre des 200 milliards d'euros. Conséquence de cette baisse progressive des investissements, la hiérarchisation des outils de défense est évidente en Europe. Hormis la France et le Royaume-Uni, la très grande majorité des pays européens ne disposent que de forces militaires locales, destinées à intervenir dans leur propre pays. Au mieux des pays comme l'Allemagne ou l'Italie ont généré des forces militaires de taille régionale susceptibles d'apporter un appui aux opérations militaires dans un rayon limité en Europe.

Au bilan, « il y a des puissances européennes mais l'Europe n'est pas à l'origine un projet de puissance »⁽¹¹⁾. Dans ce contexte et confrontée à la menace terroriste, l'Europe est soumise à de nouvelles vulnérabilités concernant sa sécurité : « Avec l'irruption du djihadisme militarisé, le fait guerrier s'importe désormais au cœur du territoire européen, que l'on pensait pourtant sanctuarisé. (...) Une rupture grave et sans nul doute durable de la situation d'insularité stratégique dans laquelle semblait nous placer la fin de la guerre froide »⁽¹²⁾.

Une Europe menacée par un monde multipolaire

Des affrontements de nouvelle nature, des guerres aux multiples visages

Des lignes de fracture apparaissent entre des zones abandonnées d'un côté (comme une large partie de l'Afrique ou du Moyen-Orient), et d'autres où s'affrontent directement ou indirectement des États forts guidés par une forme nouvelle ou renouvelée d'impérialisme. Ces lignes de fracture voient se développer une sorte de privatisation des conflits (en particulier dans les États faillis) d'une part, et une guerre d'usure d'autre part, sans vainqueurs clairement identifiés. Mais elles portent surtout en germe des risques d'affrontement beaucoup plus violents et brutaux entre les États-puissances eux-mêmes (la mer de Chine est symptomatique de ce type d'affrontement indirect qui pourrait dégénérer).

La guerre moderne a donc muté et se révèle aujourd'hui sous plusieurs formes. La guerre d'ingérence est la première évolution depuis la fin de l'ère coloniale. Avec les conséquences souvent malheureuses du prix fort payé par les populations civiles.

(10) A. MERKEL, Sommet de l'UE à Malte, 3 février 2017.

(11) H. VÉDRINE, *Le Monde*, 13 janvier 2017.

(12) J-Y. LE DRIAN, *Qui est l'ennemi ?*.

La défense du territoire européen,
enjeu de la décennie à venir pour la France ?

La question est désormais de savoir si l'ingérence restera consubstantielle à l'Occident. La deuxième est économique, comme l'illustre la faiblesse des entreprises européennes face au *diktat* du droit juridique américain ⁽¹³⁾. La troisième revisite les principes de la guerre froide : ne pas se combattre et ne pas se parler, comme c'est le cas actuellement au Moyen-Orient par théâtres interposés (Yémen, Syrie) entre l'Arabie saoudite et l'Iran. La quatrième est civile et tout aussi sanglante, engendrant des migrations internes massives (Afrique) mais également externes (Méditerranée, Europe de l'Est). Celle-ci est sans doute la plus difficile à maîtriser car elle repose sur l'ethnique et le religieux, facteurs d'affrontement de plus en plus violents, en particulier quand ce dernier repose sur le terrorisme. Sans compter la guerre nucléaire dans sa forme dissuasive et la prolifération galopante qui lui est liée, le retour des impérialismes (Iran, Turquie, Russie) quels que soient leurs motifs (économique, politique, culturel) ou la cyberguerre.

Ces nouvelles formes de la guerre ont pour conséquence d'accélérer la déliquescence des États les plus faibles et la multiplication de zones grises, au sein desquels l'influence de nations intermédiaires (Iran, Turquie, Arabie saoudite, Inde) devient prépondérante.

***Un positionnement américain imprévisible générant de l'incertitude,
fondé depuis plusieurs années sur le repli***

L'arrivée au pouvoir de la nouvelle administration américaine est sans doute l'expression de la poursuite de l'effondrement du monde bipolaire, commencé en 1991 avec la fin de l'URSS, permettant aux formes de guerre décrites précédemment de se développer.

Donald Trump s'inscrit dans la continuité de son prédécesseur quand il considère que les États-Unis ne sont plus en mesure d'être les gendarmes du monde. Néanmoins, sa victoire a ajouté un trouble supplémentaire en Asie du Sud-Est sur la survie d'accords militaires noués parfois depuis plus de 60 ans : le Président américain a ainsi laissé entendre que le Japon et la Corée du Sud auraient intérêt à se doter de l'arme nucléaire pour assurer eux-mêmes leur protection. Il a aussi menacé de remettre en cause les traités de défense avec ses alliés historiques, notamment en Europe, s'ils ne contribuaient pas davantage aux dépenses militaires.

Le pivot vers l'Asie du Sud-Est, lancé par Barack Obama en 2011, visait à resserrer les liens avec ses alliés et à réaffirmer sa domination contestée par la Chine tout en se retirant des théâtres extérieurs au Moyen-Orient (Irak, Afghanistan), se détournant ainsi de l'Europe. Ce programme ambitieux « n'a toutefois jamais vraiment convaincu les pays d'Asie du Sud-Est » ⁽¹⁴⁾. Pékin n'a pas renoncé à ses prétentions territoriales sur la quasi-totalité de la mer de Chine occidentale et a continué à aménager des îlots pour y construire des infrastructures portuaires et aéronavales. Les États-Unis se sont également montrés incapables de freiner l'escalade nucléaire nord-coréenne.

(13) La BNP a été formellement condamnée à une amende record de près de 8 Mds € en 2014 par la justice américaine pour ne pas avoir respecté l'embargo américain entre 2000 et 2010 vis-à-vis de Cuba, la Libye, le Soudan et l'Iran.

(14) Sophie BOISSEAU DU ROCHER (chercheur à l'Ifri) cité par C. PLUYETTE : « Trump va-t-il achever d'enterrer le "pivot" vers l'Asie d'Obama ? », *Le Figaro*, 13 novembre 2016.

Ils ont laissé le Moyen-Orient dans l'état que l'on connaît actuellement, avec l'obligation d'y revenir aussitôt (Irak)...

Si le retrait progressif des États-Unis pour le règlement des affaires internationales n'est pas nouveau – illustré par la politique du « *Lead from behind* », chère au président Obama, et l'échec cuisant de celui-ci au Proche-Orient – ils se démarquent désormais par l'imprévisibilité de la nouvelle administration et génèrent une incertitude anxiogène chez les Européens, accentuant ainsi leurs dissensions internes. En formalisant sa politique par le slogan « *America first* », elle confirme ce repli sur soi, et avec lui l'ensemble du monde occidental, laissant ainsi un peu plus la place à l'expansionnisme des États-puissances comme la Russie et la Chine.

La Russie, chef de file des États-puissances sur le front Est de l'Europe, en quête d'une plus forte implantation en Méditerranée et marquant son retour en Atlantique

L'intervention russe en Syrie, première opération lancée à l'extérieur de l'ancienne zone soviétique, prouve à quel point l'ancienne Armée soviétique s'est modernisée et renforcée depuis la réforme lancée en 2008 pour combler les lacunes révélées par les guerres de Tchétchénie et de Géorgie : « L'engagement syrien aurait été impossible il y a dix ans. Jusqu'à l'annexion de la Crimée en mars 2014, l'armée russe n'était plus un acteur international. L'instrument militaire, même s'il a toujours conservé son potentiel de destruction et ses capacités nucléaires, ne pouvait pas être utilisé à l'extérieur des frontières de la Russie »⁽¹⁵⁾. En quelques années, le prestige de la Russie s'est donc considérablement redressé.

Sa détermination à recourir à la force et sa rapidité à traduire la volonté politique au niveau militaire ont surpris les Occidentaux en Syrie. Préoccupées par la radicalisation d'une partie de leur population de religion musulmane (20 millions sur 140 M de Russes), les autorités russes ont engagé une grande partie de leurs moyens militaires en Irak et en Syrie, en lien avec les Iraniens et le *Hezbollah* libanais. Cette diplomatie volontariste au Moyen-Orient n'est pas nouvelle : Vladimir Poutine inscrit son action dans la continuité de la stratégie des tsars, dictée par la géographie au cœur de laquelle le domaine maritime est un enjeu afin de ne pas rester enclavé. Winston Churchill disait déjà en parlant de la Russie : « C'est un géant auquel on a bouché les narines ».

À l'avenir, c'est la politique russe dans les Balkans qui doit être l'objet de toute notre attention. La présence russe en Serbie, Bulgarie, Hongrie ou Slovaquie pourrait menacer la stabilité de ces pays et fragiliser encore un peu plus un territoire européen perméable. Pire, elle semble jouer à dessein dans cette région un rôle perturbateur vis-à-vis des objectifs de l'Union européenne. Comme le note le président du Conseil russe de politique étrangère et de défense, un centre de réflexion influent, « il y a chez nous un courant qui plaide pour un retour dans cette région »⁽¹⁶⁾.

(15) Bettina RENZ (chercheur à l'Université de Nottingham) citée par I. LASSERRE : « La puissance militaire retrouvée de la Russie », *Le Figaro*, 30 novembre 2016.

(16) Fedor LOUKIANOV cité par *Le Point*, 12 janvier 2017.

La défense du territoire européen,
enjeu de la décennie à venir pour la France ?

Déjà présente en Méditerranée orientale, notamment grâce à sa base navale permanente à Tartous (Syrie), la Russie s'efforce par ailleurs d'établir des relations durables avec l'Égypte ⁽¹⁷⁾, profitant de l'erreur de l'administration américaine perçue comme favorable aux Frères musulmans. Dans le domaine militaire des manœuvres entre les deux marines ont ainsi été menées en juin 2015 en Méditerranée.

La Chine pourrait développer sa politique du fait accompli en Méditerranée

La présence chinoise en Méditerranée, aux portes Sud de l'Europe, est désormais une réalité compte tenu de ses investissements massifs dans les infrastructures de transport, en particulier portuaires. Cherchant à mettre en place des mécanismes de coopération bilatérale en Europe du Sud (Chypre, Espagne, Grèce, Italie, Malte et Portugal), la politique chinoise fait porter un risque sur l'unité européenne, au moment où Bruxelles est en situation de fragilité. Développement maritime de son plan « *21st Century Maritime Silk Road* », l'implantation chinoise en Méditerranée est l'extension européenne de sa nouvelle route de la soie. La manœuvre chinoise n'est pas d'impliquer les Européens les plus influents à ses mécanismes de coopération, mais au contraire de profiter des faiblesses des pays périphériques pour asseoir sa domination économique, participant ainsi au potentiel délitement européen. La présence chinoise concerne l'ensemble du pourtour méditerranéen : au Pirée (Grèce), à Cherchell (Algérie), à Port-Saïd et Alexandrie (Égypte), à Ashdod et Haïfa (Israël), à Ambarli (Turquie) ou à Gênes et Naples (Italie). La question d'une stratégie chinoise ⁽¹⁸⁾ en Méditerranée se pose désormais clairement après les exercices militaires menés pendant dix jours en mai 2015, conjointement avec la Russie. Sa coopération avec ce pays correspond à une répartition des zones d'influence économique et à une entraide, confirmée par les exercices conjoints menés en mer de Chine en septembre 2016. Ceux-ci ont pu être interprétés comme une forme de renvoi d'ascenseur par les Chinois après l'opportunité russe d'entraînement offerte en Méditerranée en 2015.

Au-delà des aspects économiques, cette stratégie semble avant tout guidée par la nécessité d'évacuer ses ressortissants dans ces régions en cas de crise (plus de 35 000 Chinois ont été évacués de Libye en 2011, et près de 600 du Yémen en mars 2015). Pour autant, la capacité chinoise à ne pas respecter le droit international, illustrée par sa politique du fait accompli en mer de Chine, doit nous faire réfléchir sur ses intentions en Méditerranée. À l'image du développement chinois à Djibouti ⁽¹⁹⁾, il n'est pas irréaliste d'envisager la création d'une base navale chinoise en Méditerranée.

Aux portes de l'Europe du Sud, le Maghreb est en situation instable

Si le trait d'union entre les pays qui composent le Maghreb est la culture arabosphérique, la stabilité de l'ensemble s'avère plus que fragile. Plusieurs tentatives de rapprochement voire d'intégration économique et politique ont eu lieu, mais Maroc,

(17) La Russie fournit 40 % des importations de blé en Égypte et va construire la première centrale nucléaire à Dabca.

(18) Cherchant à s'imposer comme une puissance maritime, conformément au souhait de Xi Jinping, la Chine a publié un *Livre blanc* en mai 2015.

(19) Construction d'une base navale chinoise capable d'héberger *a priori* jusqu'à 10 000 personnes.

Algérie et Tunisie restent fondamentalement différents. Sans compter la Libye... Cette incertitude aux portes de l'Europe du Sud pourrait être le prochain sujet de sécurité pour l'Europe dans la décennie à venir.

En effet, au-delà de la problématique des flux migratoires en Méditerranée et des risques d'importation des contestations locales en cas d'effondrement du pouvoir en Algérie ou en Tunisie ⁽²⁰⁾, une dégradation de l'environnement sécuritaire dans ces pays pourrait conduire à une intensification des trafics à la frontière libyenne, à destination du Sahel ou de l'espace méditerranéen, et pourrait augmenter la menace terroriste. La maîtrise des risques et l'anticipation de leurs impacts potentiels sont désormais un sujet d'intérêt pour les pays européens, conscients de l'impossibilité de considérer la Méditerranée comme une frontière liquide, vide et protectrice.

Les Européens ayant déserté ces pays pour des raisons historiques, les pays du Maghreb sont par ailleurs un lieu d'expansion de la Chine et de la Russie, dans le cadre de leur stratégie en Méditerranée, mais également le nouveau lieu d'affrontement des pays du Golfe et de la Turquie. Le scénario d'un embrasement du Maghreb est réaliste, faisant augmenter de fait la menace sur le territoire européen en cas de déploiement de systèmes balistiques d'origine russe...

La Turquie, un problème de plus en plus important pour les Européens

La répression qui sévit en Turquie inquiète les Européens. En tout, quelque 100 000 personnes ont été touchées par les purges dans l'armée, la police, la justice, l'enseignement, la presse, l'administration et les entreprises. Et dans ce contexte, le Parlement turc pourrait adopter une réforme constitutionnelle en faveur d'un renforcement des pouvoirs du président Erdogan... Or, la Turquie est un pilier de l'Alliance. Deuxième armée par le nombre de ses militaires (avant les purges), elle est le quatrième contributeur aux opérations de l'Otan. Pour les Occidentaux, elle occupe une position stratégique, verrouillant l'accès à la Méditerranée *via* les détroits du Bosphore et des Dardanelles. Ancrée dans le Moyen-Orient, proche des Balkans et face à la Russie, elle est un pays clé pour la géopolitique européenne. Pour cette raison, l'Alliance y entretient de nombreuses installations militaires : la base aérienne d'Incirlik, utilisée par la coalition contre *Daech*, celle de Kürecik qui sert à la défense antimissile des Alliés et un centre de commandement à Izmir.

Depuis que la Turquie est entrée dans l'Alliance (1952), ses relations avec les autres pays membres ont toujours été instables. Contrariées par l'intervention militaire turque à Chypre en 1974, réchauffées dans les années 1990, elles se sont à nouveau dégradées au début des années 2000, lorsque l'Europe a refusé de considérer le *PKK* (Parti des travailleurs du Kurdistan) comme une organisation terroriste. Avec la guerre

(20) De nombreux binationaux et ressortissants maghrébins sont présents dans l'Union européenne : 877 398 Algériens, 414 077 Tunisiens, 3 056 109 Marocains, 66 344 Libyens. Source : Philippe Fargues, *EU Neighbourhood migration report 2013*, European University Institute.

La défense du territoire européen,
enjeu de la décennie à venir pour la France ?

en Syrie, les motifs de discorde se sont multipliés : le rapprochement avec la Russie de Vladimir Poutine jette un trouble ⁽²¹⁾.

La liste des reproches occidentaux est longue : en 2013, la décision d'Ankara de s'équiper d'un système de défense antiaérien chinois a provoqué un tollé parmi les pays de l'Otan, qui ont forcé le gouvernement turc à reculer. Depuis le début du conflit syrien, ces derniers reprochent à Ankara son ambivalence vis-à-vis de *Daech* ainsi que sa complaisance vis-à-vis de Téhéran dans le difficile règlement du dossier nucléaire iranien. Les Européens n'ont pas apprécié le chantage exercé par Ankara sur la question des migrants. Depuis, ils s'interrogent : la Turquie est-elle en train de renoncer à son ancrage occidental ?

Les griefs sont tout aussi nombreux du côté turc et sa méfiance ne date pas d'aujourd'hui. À l'époque de la guerre froide, le président américain Lyndon Johnson avait menacé de ne pas soutenir la Turquie si une crise éclatait entre Ankara et l'URSS sur la question chypriote. Sans compter le refus de l'Otan de considérer la demande de protection d'Ankara qui craignait des représailles de Saddam Hussein pendant la guerre contre l'Irak en 2003.

C'est l'absence de vision et de politique claire du monde occidental, dans la situation de désintégration de la région, qui pousse Ankara à se forger de nouvelles alliances : « L'entente avec la Russie est fondée sur le désespoir » ⁽²²⁾.

Concentrer ses efforts sur la défense du territoire européen

La poursuite du développement multipolaire des relations dans le monde révèle donc que celui-ci est désormais dominé par trois pays (États-Unis, Chine, Russie), alors que des zones grises (Moyen-Orient, Afrique, Balkans...) cherchent leur place, hésitant entre rallier brutalement ces États-puissances ou tenter de s'en remettre à des pays émergents de taille intermédiaire qui s'émancipent (Inde, Iran...) grâce à leurs ressources énergétiques, à leur position géostratégique ou à leur puissance nucléaire (quand ils ne possèdent pas les trois...).

Dans ce monde déstructuré, l'Europe joue de plus en plus le rôle de spectateur, fragilisée par ses incohérences internes à l'image de son incapacité à peser en Syrie : « aujourd'hui, les Européens, qui croyaient vivre dans le monde idéal de la communauté internationale et du droit, se réveillent dans Jurassic Park : Donald Trump inquiète tout le monde, Poutine nous provoque, l'Islam se convulse » ⁽²³⁾.

(21) Dans l'accord passé entre Moscou et Ankara, la Russie aurait donné son feu vert à une sorte de zone de sécurité dans le Nord de la Syrie qui empêcherait les Kurdes du PYD d'y installer une région autonome. En échange, Ankara aurait levé son *вето* au maintien au pouvoir de Bachar el-Assad, l'allié de la Russie. Cette coopération a franchi une nouvelle étape quand les avions russes ont mené des frappes pour soutenir l'offensive de la Turquie dans le Nord de la Syrie.

(22) B. BALCI cité par I. LASSERRE *op. cit.*

(23) H. VÉDRINE, *Le Monde, op. cit.*

La défense du territoire européen,
enjeu de la décennie à venir pour la France ?

Or, le monde se recompose à ses frontières, et les tensions se rapprochent inexorablement de son territoire : le Maghreb, le Moyen-Orient ⁽²⁴⁾ ou l'Europe de l'Est sont désormais le lieu d'affrontements directs ou indirects et des jeux d'influence des États-puissances.

Développer une capacité de « démonstration de puissance » européenne dans le haut du spectre

Dans le cadre de sa politique de défense, la France devra prendre en compte dans la décennie à venir le besoin d'une capacité de « démonstration de puissance » européenne en mesure de répondre aux rapports de force que ces États-puissances veulent imposer aux Européens par leur stratégie du fait accompli, dont l'objectif n'est pas d'aller à l'affrontement mais de s'imposer régionalement. La formalisation en France d'une telle fonction stratégique lui permettrait de préciser ses positions au sein de l'Alliance atlantique et de mieux se faire comprendre de ses partenaires, pour une meilleure cohésion européenne et un niveau d'ambition cohérent face aux menaces émergentes.

La tentation de poursuivre exagérément nos interventions loin du territoire national pour le combat contre le terrorisme islamique – qui risque à tout moment et dans la durée de se manifester contre nos propres concitoyens – pourrait nous entraîner vers un investissement capacitaire dédié et nous faire négliger le besoin de capacités terrestres en nombre dans le haut du spectre nécessaires à toute forme de démonstration de puissance : « L'armée française a été transformée en un kit expéditionnaire » ⁽²⁵⁾. Ces capacités seront de plus en plus sollicitées pour faire face aux menaces puissantes aux frontières européennes, à l'image des nouveaux contrats « *Enhanced Forward Presence* » définis par l'Otan dont l'objectif est de prépositionner des forces en Europe.

Les espaces maritimes seront sans doute un lieu majeur d'expression de cette démonstration de puissance européenne, indispensable à la préservation de ses intérêts, allant bien au-delà des problèmes de gestion des flux migratoires. En effet, la multiplication des patrouilles sous-marines suspectes à la limite des eaux européennes (Atlantique, Méditerranée), le développement des marines asiatiques (Chine, Russie) en Méditerranée et la situation très volatile des pays du Maghreb (Algérie, Tunisie, Libye) ou du Proche-Orient (Syrie) laissés à l'influence de la Chine ou de la Russie nécessitent de développer des capacités navales militaires du haut du spectre pour être en mesure de protéger dans la durée le sanctuaire européen. Or à l'horizon 2030, le paysage naval mondial aura été totalement renouvelé, fruit d'un investissement colossal (40 Mds de dollars chaque année dont 12 Mds pour les États-Unis et autant en Asie). Les flottes sont donc de plus en plus symétriques, avec une forte poussée des

(24) L'Iran a annoncé avoir mené des exercices militaires, incluant des tirs de missiles balistiques le 29 janvier 2017, en réaction aux sanctions américaines concernant l'immigration en provenance de pays musulmans. Or, les accords sur le programme nucléaire iranien sont sans doute le meilleur exemple d'une forme d'apaisement international, désiré par le président Obama et les Européens, après les interventions en Afghanistan et en Irak.

(25) « Entretien avec le général (2S) Vincent DESPORTES », ASAF, 9 février 2017.

outils de premier rang (porte-avions ou porte-aéronefs, bâtiments amphibies, sous-marins).

Dans un autre domaine, la multiplication des vols de démonstration de la part de l'aviation stratégique russe (bombardiers Tu-160 Blackjack dédiés à l'arme nucléaire) en 2016, et plus récemment en février 2017, nous prouve à quel point la sanctuarisation du territoire européen (et de son espace aérien) est fragile et reste un enjeu majeur. Allant bien au-delà des incursions de l'aviation russe dans le ciel des États baltes, ces démonstrations régulières rappellent à tous les Européens que la protection de l'ensemble de leur territoire nécessite des capacités importantes et une coopération de tous les instants. Or, le « mitage » des outils européens de défense antiaérienne constitue une fragilité importante dans le haut du spectre capacitaire : les aviations européennes s'écroulent, la plupart des flottes de l'Europe de l'Est étant à bout de souffle, avec des coûts de renouvellement exorbitants, poussant les Nations concernées à vouloir financer en commun les nouvelles capacités.

Repenser la fonction stratégique « protection » à l'échelle européenne

Les contraintes financières imposées par la situation compliquée de la plupart des budgets européens (due à une économie atone) nécessitent de développer dans la décennie à venir une approche européenne volontariste pour faire face aux risques d'implosion d'une part, et aux menaces qui se développent à la périphérie de l'Europe d'autre part.

Pourtant, les fuites récentes dans la presse britannique ⁽²⁶⁾ d'une note émanant de l'ancien commandant du Commandement des forces interarmées britanniques, le général *Sir* Richard Barrons, indiquent que l'Otan, fragilisée par les divisions entre ses membres, ne serait pas en mesure de réagir en cas d'agression russe.

Le défi est donc celui du financement de la défense de l'Europe, que les Alliés européens se sont refusé jusqu'à présent de relever. Dans ce contexte, une partie d'entre eux rêvent de financer en commun leurs capacités les plus onéreuses. Or, ce type d'investissement fait porter un risque réel de tétanie opérationnelle en cas de besoin : pour engager des capacités communes, les Nations doivent unanimement porter des objectifs politiques et militaires communs, ce qui est compliqué lors des interventions en coalition internationale ⁽²⁷⁾.

Au contraire, les Européens doivent développer en propre les capacités du haut du spectre qu'ils sont en mesure de mettre à disposition de leurs partenaires dans le cadre de coalitions *ad hoc* lorsque leurs intérêts politiques convergent.

Pour inciter ses partenaires européens à aller dans ce sens, la France doit donner des gages en participant dans la durée au fardeau de la défense du territoire européen, hors du champ de sa dissuasion nucléaire. Tout en préservant sa capacité de

(26) D. HAYNES, *The Times*, 19 septembre 2016.

(27) En Afghanistan, l'engagement des AWACS de l'Otan n'a pas été possible au début de l'intervention de l'Otan faute d'accord de l'Allemagne.

projection et d'entrée en premier (Afrique, océan Indien, sans oublier la zone Pacifique). Cela nécessitera, dans la décennie à venir, des investissements clairs dans notre outil de défense pour récupérer des marges de manœuvre, notamment numériques.

Dans ce contexte, il est souhaitable de redéfinir précisément la fonction stratégique « protection » en l'élargissant au territoire européen. Un nouvel exercice de réflexion stratégique impliquant fortement nos principaux partenaires européens (Royaume-Uni, Allemagne mais également Italie, Espagne, Pays-Bas, Belgique, Norvège, Pologne) doit être mené afin de définir conjointement les moyens et capacités à générer pour la protection de l'Europe. Cette réflexion devra prendre en compte le futur de l'offre américaine de défense antimissile balistique, mise à la disposition de l'Alliance atlantique ⁽²⁸⁾ dans le cadre de la protection des États-Unis. En effet, l'incertitude générée par l'arrivée de la nouvelle administration américaine devrait faire évoluer les positions de certains partenaires européens sur la fiabilité politique d'un tel dispositif de protection qui, de surcroît, risque de détourner une partie de leurs moyens, notamment navals, pour la protection des installations américaines en Europe.

Pour cela, le maintien d'une relation forte avec le Royaume-Uni, libéré de son dilemme vis-à-vis de l'Europe de la défense quand sa sortie de l'UE sera effective, est un enjeu majeur afin d'envisager une forme de pilier européen au sein de l'Alliance : « Je suis fier du rôle que la Grande-Bretagne a joué et continuera à jouer pour la sécurité de l'Europe. Elle a été *leader*, en Europe, pour maintenir notre continent en sûreté, que ce soit pour mettre en œuvre des sanctions contre la Russie après son action en Crimée, ou pour assurer la paix et la stabilité dans les Balkans, ou pour protéger la frontière extérieure de l'Europe. Nous allons continuer à travailler en étroite collaboration avec nos alliés européens en matière de politique étrangère et de défense alors même que nous quittons l'UE elle-même » ⁽²⁹⁾.

Une dissuasion française qui sanctuarise la démonstration de puissance européenne

Les démonstrations russes aux portes du territoire européen reposent sur le principe de la sanctuarisation agressive dont l'ambition est de réaliser un fait accompli indiscutable fondé soit sur la vitesse et la surprise (gesticulations maritimes et aériennes en espace international), soit sur des manœuvres combinant la subversion, le terrorisme ou l'insurrection (Ukraine).

Cette nouvelle doctrine russe augmente le nombre de scénarios dans lesquels l'arsenal nucléaire pourrait être employé. À l'époque de la guerre froide les règles tacites qui régissaient les armes nucléaires étaient respectées. Ce n'est plus le cas : « la manière dont les Russes utilisent l'arme nucléaire brouille le jeu traditionnel entre la dissuasion qui normalement sert à la protection des intérêts vitaux et la coercition. La menace nucléaire est utilisée non plus pour consolider un *statu quo* mais pour le changer. (...) Si elle nous empêche (...) d'apporter une réponse conventionnelle à un problème,

(28) *European Phased Adaptive Approach*, montée en puissance d'ici 2018 d'un dispositif de défense antimissile balistique en Europe reposant sur les systèmes américains Aegis, installés à bord de frégates et destroyers américains basées à Rota (Espagne), et à terre en Pologne et en Roumanie.

(29) T. MAY, 17 janvier 2017.

La défense du territoire européen,
enjeu de la décennie à venir pour la France ?

la Russie nous force à nous placer un jour, nous aussi, dans une logique d'emploi de l'arme nucléaire »⁽³⁰⁾.

Ainsi, lorsqu'il menace d'utiliser son arsenal stratégique pour traiter des sujets comme l'Ukraine, que l'Occident considère comme étant séparés du nucléaire, Vladimir Poutine fait monter d'un cran la menace. L'Europe doit donc bâtir une doctrine capable de préserver ses marges de manœuvre de sorte qu'elle puisse d'une part sonder les intentions des acteurs et d'autre part, leur signifier de façon explicite un seuil à ne pas dépasser : « Les Européens oublient la grammaire de la dissuasion car elle appartient selon eux aux temps anciens de la guerre froide. Mais la fluidité de plus en plus grande entre la force conventionnelle et l'arme nucléaire fait courir au monde un grand danger »⁽³¹⁾.

Jusqu'à présent, trois pays (États-Unis, Royaume-Uni et France) en Occident pouvaient s'appuyer sur leur dissuasion nucléaire pour maintenir un effet de seuil nucléaire élevé pour la stabilisation de leur zone géographique et le respect de leurs intérêts dans le monde. Or, la politique « *America first* » affichée par le président Trump révèle l'incertitude quant à la volonté américaine de vouloir maintenir son niveau d'intervention au profit des Occidentaux. Quant au Royaume-Uni, fatigué par une dizaine d'années de déploiements extérieurs (Afghanistan et Irak), son repli politique ne peut être nié, fragilisant de fait sa capacité d'intervention. En attendant d'être en mesure de disposer d'un outil militaire à nouveau à la hauteur de ses ambitions. En outre, la dépendance britannique de plus en plus assumée vis-à-vis des Américains dans le contexte du *Brexit* participe à faire chuter son seuil d'intervention. La France pèse donc de façon très singulière dans le dispositif européen. Elle est actuellement la seule en mesure d'offrir de façon autonome, comme Nation européenne, une dissuasion permettant de maintenir un seuil nucléaire élevé face aux adversaires potentiels de l'Europe. Par sa capacité à se positionner en appui des pays européens, elle contribue directement à la sécurité collective.

Face aux menaces décrites précédemment, la crédibilité de la dissuasion nucléaire permet de sonder les intentions des adversaires, c'est-à-dire de pouvoir mettre des moyens sur la table d'une crise. C'est tout l'enjeu de la démonstration de puissance européenne pour la sanctuarisation du territoire européen. Cela permet de bâtir un dialogue stratégique en dessous du seuil nucléaire, pour éviter le fameux « dilemme du tout ou rien »⁽³²⁾. Cela exige des capacités classiques d'une quantité et d'un niveau suffisants puis de les déployer pour obliger l'adversaire à discuter. Cette réflexion doctrinale et capacitaire doit désormais être menée au niveau européen suivant les termes du communiqué du Sommet de Varsovie ayant réaffirmé la dimension nucléaire de l'Alliance⁽³³⁾. Sans renoncer pour autant à notre autonomie stratégique.

(30) C. BRUSTLEIN (Ifri) cité par I. LASSERRE, « Périls nucléaires, le retour ? », *Le Figaro*, 13 février 2017.

(31) C. BRUSTLEIN, *op. cit.*

(32) Cf. la stratégie atomique d'André BEAUFRE cité par G. CHALIAND, *Anthologie mondiale de la Stratégie*, p. 1472.

(33) « Aussi longtemps qu'il y aura des armes nucléaires, l'Otan restera une alliance nucléaire. (...) Les forces nucléaires stratégiques indépendantes du Royaume-Uni et de la France (...) contribuent à la sécurité globale de l'Alliance. L'Alliance assurera une participation aussi large que possible des Alliés concernés aux arrangements agréés pour le partage du fardeau dans le domaine nucléaire ». Déclaration des chefs d'État et de gouvernement du Sommet de Varsovie des 8 et 9 juillet 2016.

Conclusion

Dans un monde incertain, complexe et fortement évolutif, la doctrine nucléaire doit être globale. C'est la dimension européenne de la dissuasion française, par l'effet de seuil qu'elle garantit, qui permettra dans l'avenir aux Européens d'assurer par eux-mêmes la protection de leur territoire et de maintenir leur liberté d'intervention au-delà pour la défense de leurs intérêts partagés. Elle repose en amont sur la capacité européenne à démontrer sa puissance dans ses zones d'intérêt afin de rééquilibrer le rapport de force avec les États-puissances et les Nations émergentes.

Protection, démonstration de puissance et dissuasion nucléaire formeront le triptyque de la politique de défense européenne dans la décennie à venir.

Éléments de bibliographie

Ouvrages

- CHALIAND Gérard, *Anthologie mondiale de la Stratégie*, Bouquins, 2009 ; 1632 pages.
- DEL VALLE Alexandre, *Les vrais ennemis de l'Occident – Du rejet de la Russie à l'islamisation des sociétés ouvertes* ; Éditions de l'Artilleur, 2016 ; 541 pages.
- Dossier « France-Russie, d'hier à aujourd'hui », *Espoir* n° 185, Revue de la Fondation Charles de Gaulle, décembre 2016.
- GIRARD Renaud, *Le monde en guerre – 50 clefs pour le comprendre* ; Carnets Nord – Édition Montparnasse, 2016 ; 360 pages.
- HUNTINGTON Samuel, *Le choc des civilisations* ; Odile Jacob, 1997 ; 547 pages.
- LE DRIAN Jean-Yves, *Qui est l'ennemi ?* ; Les Éditions du Cerf, 2016 ; 76 pages.
- MONTBRIAL (de) Thierry et DAVID Dominique, *Ramses 2017 – Un monde de ruptures* ; IFRI, Éditions Dunod, 2016 ; 350 pages.
- Dossier « À l'Est, rien de nouveau ? », *Revue Défense Nationale* n° 795, décembre 2016.
- VÉDRINE Hubert, *Sauver l'Europe* ; Éditions Liana Levi, 2016 ; 94 pages.
- VILLEPIN (DE) Dominique, *Mémoires de paix pour temps de guerre* ; Éditions Grasset & Fasquelle, 2016 ; 665 pages.

Presse

- « Entretien avec le général (2S) Vincent DESPORTES : "L'armée a été transformée en un kit expéditionnaire" », Association de soutien à l'armée française, 9 février 2017.
- GIRARD René, « Le cadeau de Trump à l'Union européenne », *Le Figaro*, 30 janvier 2017.
- HAYNES Deborah, « NATO has no plan if Russia invades, warns ex-general », *The Times*, 19 septembre 2016.
- LASSERRE Isabelle, « Périls nucléaires, le retour ? », *Le Figaro*, 13 février 2017.
- LASSERRE Isabelle, « La défiance s'installe entre l'Otan et Ankara », *Le Figaro*, 26 janvier 2017.
- LASSERRE Isabelle : « La puissance militaire retrouvée de la Russie », *Le Figaro*, 30 novembre 2016.
- PLUYETTE Cyrille : « Trump va-t-il achever d'enterrer le "pivot" vers l'Asie d'Obama ? », *Le Figaro*, 13 novembre 2016.
- « Hubert Védrine : "En Occident, l'heure est venue d'un inventaire sérieux sur nous-mêmes" », *Le Monde*, 13 janvier 2017.
- HOLLANDE François, Sommet des chefs d'État et de gouvernement de l'UE, 3 février 2017.
- MERKEL Angela, Sommet de l'UE à Malte, 3 février 2017.
- TUSK Donald, Sommet des chefs d'État et de gouvernement, 3 février 2017.
- MAY Theresa, 17 janvier 2017.

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?

Quelles conséquences stratégiques pour la défense européenne ?

Bertrand JARDIN

| Colonel (air), auditeur de la 66^e session du Chem.

La présence militaire américaine en Europe : perspective historique et données contemporaines

De la guerre froide au « pivot vers l'Asie » : les chiffres d'un désengagement militaire d'Europe

Après une phase de consolidation dans les années 1950, la présence militaire américaine sur le continent européen a connu une nette diminution dès la fin de la période de la guerre froide reflétant l'évolution favorable de la situation géostratégique régionale.

Sur fond de tensions croissantes entre les États-Unis et l'Union soviétique, les années d'après-guerre connaissent une montée en puissance rapide des troupes américaines stationnées en Europe concomitamment avec la signature, en avril 1949, du Traité de l'Atlantique Nord. Les effectifs passent ainsi de 120 000, à la fin de la guerre, à 400 000 militaires en 1953 ⁽¹⁾ marquant la détermination américaine à s'opposer à toute agression militaire soviétique en Europe et renforçant ainsi la crédibilité de l'Article 5 ⁽²⁾, fondement même du Traité de l'Atlantique Nord.

Au début des années 1970, sous la pression de l'engagement militaire au Vietnam, les États-Unis procèdent à une bascule d'efforts. Le volume des forces armées américaines stationnées en Europe diminue alors progressivement pour atteindre 265 000 hommes. Ce désengagement partiel d'Europe est toutefois temporaire.

À la fin des années 1970, en réponse au déploiement par l'Union soviétique de missiles balistiques de portée intermédiaire, SS-20, en Europe de l'Est, les États-Unis déploient, dans le cadre de l'Organisation du Traité de l'Atlantique Nord (Otan),

(1) L'armée de l'air américaine passe de 3 groupes (35 000 personnes) à 12 escadres (136 000 personnes). La 6^e Flotte en Méditerranée double pour atteindre 40 navires de guerre. L'armée de terre américaine passe d'une division d'infanterie et 3 régiments de maréchaussée à 2 corps d'armée, composés de 5 divisions, coiffés par la 7^e Armée.

(2) L'Article 5 du Traité de l'Atlantique nord stipule que « les pays membres conviennent de considérer une attaque armée contre l'un d'eux, en Europe ou en Amérique du Nord, comme une attaque dirigée contre tous ».

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

des missiles de portée intermédiaire Pershing II ainsi que des missiles de croisière sol-sol (*Ground Launched Cruise Missiles*), confirmant une nouvelle fois leur engagement aux côtés des Européens et par là même la vitalité de l'Alliance.

À la fin des années 1980, les forces du commandement américain en Europe étaient constituées de près de 350 000 hommes ⁽³⁾ réparties dans pas moins de 1 421 installations. Pour les seules forces terrestres, l'Otan comptait alors près de 8,5 millions de soldats équipés de près de 61 000 chars de combat et pièces d'artillerie face aux 7,5 millions d'hommes et aux 145 000 blindés et canons du Pacte de Varsovie ⁽⁴⁾.

À partir de 1989, la chute des régimes communistes met un terme à cet impressionnant rapport de forces : la majorité des unités est rapatriée ou dissoute. La présence américaine diminue alors rapidement pour atteindre, en 2000, le chiffre de 120 000 puis, en 2012, de 80 000 militaires stationnés en Europe. En raison, d'une part de coupes budgétaires et d'autre part, de la réorientation de la stratégie américaine vers la région Asie-Pacifique, les réductions se poursuivent ; ainsi, l'*US Air Force* diminue progressivement son empreinte au Portugal et au Royaume-Uni.

Au-delà de ces chiffres, le désengagement est marqué par une évolution de la nature des forces américaines stationnées en Europe. Ainsi, en 2013, le 5^e Corps d'armée (*US Army*) est désactivé à son retour d'Afghanistan, où il avait été déployé l'année précédente, laissant le commandement américain en Europe sans état-major de niveau de corps d'armée pour la première fois depuis 1951. Le 31 mai 2013, la *172nd Infantry Brigade* basée à Grafenwöhr (Bavière), est dissoute. L'Europe ne compte alors plus de formations blindées/mécanisées américaines sur son sol.

**Crise russo-ukrainienne :
le désengagement marque une pause**

L'absence de formations blindées est toutefois de courte durée car, avec la crise russo-ukrainienne, les chars américains font leur retour sur le sol européen, dès janvier 2017, dans le cadre des mesures dites de réassurance sur le flanc Est de l'Alliance. L'opération *Atlantic Resolve*, concrétisation de l'initiative américaine de réassurance européenne (*European Reassurance Initiative*) décidée en 2014, prévoit de fait qu'une brigade blindée soit présente en permanence en Europe ⁽⁵⁾.

À partir de 2014, on assiste donc à une inflexion de la courbe de déflation initiée à la disparition de l'Union soviétique. Ainsi, malgré la réduction du nombre de forces américaines stationnées en permanence en Europe, les effectifs – plus de 60 000 hommes – restent-ils sensiblement stables à la faveur du déploiement périodique de troupes américaines (environ 4 000 hommes) dans le cadre des mesures de « présence avancée renforcée » (*enhanced forward presence*) décidées au Sommet de

(3) UNITED STATES EUROPEAN COMMAND, « History » (www.eucom.mil/about/history/history).

(4) État-major militaire international de l'Otan, « Les origines de la structure militaire de l'Otan : de la création de l'Alliance à la chute du Mur de Berlin », *Questions militaires* n° 1, 2006.

(5) Ce plan est réalisé par rotations successives, chaque brigade étant basée en Europe de l'Est durant une période, en principe de 4 à 9 mois, afin d'y accomplir des entraînements et des exercices avec les partenaires locaux de l'Otan.

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

Varsovie (2016). Nous sommes toutefois loin du demi-million enregistré au plus fort de la guerre froide.

Point notable, cette nouvelle brigade blindée américaine n'est pas « stationnée » en permanence, mais est déployée par rotations successives et constituée d'unités basées à l'extérieur de l'Europe. Un tel déploiement présente l'avantage de rassurer les alliés, sans s'engager dans la durée ni remettre en cause l'acte fondateur sur les relations entre l'Otan et la Fédération de Russie (signé à Paris en 2009). La flexibilité d'un tel dispositif rend en outre possible une bascule d'efforts vers un autre point du globe.

Cette évolution du dispositif militaire américain s'est accompagnée, au cours de la dernière décennie, d'un glissement progressif de son centre de gravité vers l'Europe centrale et orientale, concrétisant en outre une stratégie d'influence vers de nouveaux alliés soucieux de bénéficier du bouclier américain, seul capable à leurs yeux de les protéger de la menace potentielle russe. L'implantation, en Roumanie et en Pologne, du futur dispositif fixe de défense antimissile de l'Alliance, composé de radars et d'intercepteurs exo-atmosphériques renforce cette tendance.

Ainsi, au rythme des tensions Est-Ouest et des interventions américaines, les forces stationnées en Europe ont-elles été appelées à jouer un triple rôle d'assurance de la solidarité américaine en cas d'agression soviétique puis russe (donc un rôle à la fois stabilisateur et dissuasif vis-à-vis de cette menace potentielle), de point d'appui permettant la projection de forces vers les zones de crise et de réservoir de forces pour ces différents théâtres d'opérations.

L'analyse des fluctuations de la présence militaire américaine fait ressortir une tendance de fond, celle d'un désengagement progressif, traduction de l'évolution de la place de l'Europe dans la stratégie globale américaine.

**Place de l'Europe dans la stratégie globale américaine :
du « centre de gravité » à la « masse de manœuvre »**

La complexité des relations entre États-Unis et l'Europe

Henri Kissinger écrivait à propos de la relation transatlantique : « La question de la nature de la relation qu'entretiennent les deux côtés de l'Atlantique pose celle de l'identité de l'Europe en particulier sur la scène internationale ». La relation entre

Répartition des 46 bases américaines en Europe (source : Militarybases.com)

Nombre de bases	Pays	Nombre de bases	Pays
20 (2 <i>US Air Force</i> , 1 mixte et 17 <i>US Army</i>)	Allemagne	2 (<i>USAF</i>)	Turquie
7 (4 <i>US Navy</i> , 2 <i>US Army</i> , 1 <i>USAF</i>)	Italie	2 (1 <i>US Navy</i> + 1 <i>USAF</i>)	Espagne
6 (<i>USAF</i>)	Royaume-Uni	2 (1 <i>US Army</i> et 1 mixte)	Pays-Bas
4 (1 <i>US Army</i> , 3 <i>USAF</i>)	Bulgarie	1 (<i>US Navy</i>)	Grèce
2 (<i>US Army</i>)	Belgique	1 (<i>US Army</i>)	Kosovo

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

l'Europe et les États-Unis reste complexe en raison notamment des difficultés qu'ont les Américains à comprendre des modes de décision et un système européen souvent illisibles. Le même Henri Kissinger s'interrogeait ainsi : « Qui dois-je appeler ? » ⁽⁶⁾.

Pour la plupart des Américains, l'Europe est en effet lointaine. Les États-Unis, pays à l'échelle d'un continent et en grande partie autosuffisant, n'ont pas, pendant longtemps, éprouvé le besoin de regarder ailleurs, ni de commercer avec le reste du monde : en 2010, les exportations ne représentaient que 10 % du PIB. Si l'Europe est évoquée périodiquement par les médias, c'est de façon anecdotique, à l'occasion d'un Sommet du G20, mais jamais sur le fond de la construction européenne.

Pour les États-Unis, seule l'Europe économique et commerciale existe véritablement. Après avoir aidé l'Europe à se redresser en 1945, les entreprises sont désormais à la fois partenaires et concurrentes, le règlement des différends étant assuré par l'OCDE (Organisation de coopération et de développement économiques). Le feuilletton de l'appel d'offres, portant sur le remplacement des avions ravitailleurs de l'*US Air Force* en 2011, illustre à cet égard la volonté américaine de préserver avant tout ses propres intérêts. Dans le cadre du règlement des crises économiques, les positions divergent souvent entre les deux rives de l'Atlantique, l'Europe privilégiant l'emploi de la réglementation, ce qui n'est pas nécessairement le cas aux États-Unis, fondamentalement ancrées dans le libéralisme.

Dans le domaine militaire, l'Europe n'existe pas en tant que telle ; pour Washington, elle est essentiellement assimilée à l'Otan et donc constituée des 28 États-membres. L'Europe y apparaît souvent désunie (comme pour l'Irak en 2003), une distinction étant faite – particulièrement par l'administration Bush – entre la « vieille Europe » et la « nouvelle Europe » constituée des pays d'Europe centrale et orientale (PECO). Ces derniers ont fait le choix de soutenir les États-Unis, convaincus que leur salut vis-à-vis de la Russie dépendait, sur le plan militaire, des États-Unis et non de l'Union européenne (UE). Dans ce contexte, la Turquie constitue une pomme de discorde entre les deux rives de l'Atlantique, les États-Unis ayant longtemps appuyé son entrée au sein de l'UE, en tant qu'allié stratégique, ce que certains pays européens considèrent comme une intolérable ingérence dans leur politique communautaire. L'Europe diplomatique peine également à exister aux yeux des Américains, les relations étant essentiellement bilatérales.

Au bilan, les États-Unis font 3 reproches à l'Europe : elle n'est pas assez militarisée, ne dépense pas suffisamment pour faire sa défense et n'envoie pas suffisamment de troupes en opérations.

Le rééquilibrage de la stratégie américaine vers la région Asie-Pacifique

Le concept du pivot vers l'Asie a été formalisé pour la première fois par Barack Obama dans un document publié en janvier 2012, intitulé *Sustaining Global*

(6) Anne-Emmanuelle DEYSINE, « L'Europe vue de Washington », Conférence IHEDN, 12 avril 2010 (<http://deysine.com/fr/medias/medias-radiotelevision/8-l-europe-vue-de-washington>).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

Leadership: Priorities for the 21st Century Defense ⁽⁷⁾. Il y était notamment indiqué que les États-Unis devraient « nécessairement se rééquilibrer vers la région Asie-Pacifique ».

En réalité cette évolution de la stratégie américaine n'est pas nouvelle. Depuis plusieurs années, le centre de gravité de la sécurité des États-Unis, autrefois européen, s'est déplacé vers la région Asie-Pacifique, traduction de l'évolution de la menace sur les intérêts américains telle qu'elle était perçue à Washington : d'un côté une Russie affaiblie ne présentant pas de menace directe pour la stabilité en Europe et de l'autre une Chine en pleine ascension s'imposant progressivement comme une puissance militaire capable de défier celle des États-Unis dans sa sphère d'influence ⁽⁸⁾, particulièrement dans la région Pacifique, de contester son hégémonie et d'entrer en compétition directe pour la captation de ressources naturelles dans le monde.

Dans les faits, cette bascule d'effort militaire est restée inachevée en raison de l'évolution de la situation sécuritaire au Proche et Moyen-Orient, et en Europe de l'Est, imposant la poursuite voire le réinvestissement d'un effort militaire américain dans ces régions. C'est ainsi qu'en novembre 2011, Hillary Clinton évoquait, dans un article publié dans le magazine *Foreign Policy*, la fin des coûteux conflits en Irak et en Afghanistan comme « précondition au rééquilibrage vers l'Asie » ⁽⁹⁾ tout en réaffirmant la tendance de fond : « L'avenir de la politique sera décidé en Asie, pas en Afghanistan ou en Irak, et les États-Unis seront au centre de l'action ».

Outre l'accroissement de l'engagement économique et diplomatique dans cette région, ce pivot s'est traduit, en termes militaires, par un renforcement des capacités opérationnelles de PACOM ⁽¹⁰⁾ sous la forme d'une hausse des effectifs prépositionnés, notamment au Japon, de l'ouverture de nouvelles bases et du déploiement de nouveaux moyens maritimes en mer de Chine méridionale.

La stratégie du « leading from behind » de Barack Obama à Donald Trump

Au-delà d'une vision commune idéaliste du rôle des États-Unis dans le monde, la stratégie mise en œuvre par Barack Obama reste marquée par un profond réalisme, s'inscrivant en fait dans la continuité de l'inflexion opérée par son prédécesseur dans un contexte d'enlisement des engagements militaires en Irak et en Afghanistan.

Le spectre du traumatisme vietnamien dans l'opinion publique américaine a en effet conduit George W. Bush à abandonner en 2005 la vision interventionniste et idéologique prônée par les néoconservateurs au profit d'une vision plus réaliste, se caractérisant par un désengagement militaire progressif, accompagné par une diplomatie plus affirmée, permettant ainsi un recentrage sur les intérêts nationaux. Cette bascule d'efforts devait permettre aux États-Unis de se focaliser sur les principaux

(7) *Sustaining Global Leadership: Priorities for the 21st Century Defense*, January 2012 (http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf).

(8) La Chine occupe désormais le 2^e rang mondial des dépenses en matière de défense avec 145 milliards de dollars en 2016.

(9) Hillary CLINTON, « America's Pacific Century », *Foreign Policy*, 11 October 2011 (<http://foreignpolicy.com/2011/10/11/americas-pacific-century/>).

(10) *Pacific Command* : commandement régional américain couvrant la zone Asie-Pacifique.

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

enjeux qui structurent une scène internationale désormais qualifiée de multipolaire. La montée en puissance de la Chine s'inscrit dans la ligne de mire de cette stratégie.

Le choix du maintien de Robert Gates à la tête du département de la Défense (*DoD*) illustre, à ce titre, la continuité endossée par Barack Obama. C'est ainsi que la stratégie vise à limiter l'emploi de la puissance militaire à la prise en compte des menaces immédiates. Parmi les priorités fixées au travers des *National Security Strategy* successives de 2010 et de 2015 ⁽¹¹⁾ figurent ainsi la démilitarisation du programme nucléaire iranien, l'établissement d'une nouvelle coexistence pacifique avec la Russie (synthétisée sous le terme de « reset ») et le pivot vers la région Asie-Pacifique. Dans ce contexte, la puissance militaire sert avant tout à renforcer la posture dissuasive américaine en appuyant le message de fermeté de la diplomatie tout en limitant les cas d'emploi direct de la force. Ce positionnement permet en outre de dégager des marges de manœuvres rendues nécessaires par l'exigence de redressement des comptes publics (sous la pression du *Budget Control Act* de 2011). Cette doctrine – dont l'un des principes a été formalisé sous le vocable de « *leading from behind* » – se manifeste par l'utilisation de relais de puissance à l'instar de l'engagement en Libye dont l'effort militaire principal était pourvu par la France et la Grande-Bretagne. Le chaos libyen qui s'est ensuivi, la lutte contre *Daech* et la poursuite de l'affirmation des États « puissance » chinois et russe ont conduit l'administration Obama à infléchir cette stratégie en augmentant le poids relatif de l'outil militaire.

L'élection de Donald Trump présente la perspective d'une évolution de cette stratégie sans pour autant marquer de réelle rupture. En effet, si l'on se réfère aux premières déclarations du nouveau Président, elle induit une potentielle amplification du mouvement de recentrage sur les intérêts nationaux, commencé par son prédécesseur.

Elle semble ainsi concrétiser le retour à la Maison-Blanche d'un courant conservateur tourné vers la défense exclusive des États-Unis et de leur modèle politique et social, sous-tendu par des slogans de campagne, « *America first* » et « *Make America great again* », ce qui n'est pas sans rappeler celui de Ronald Reagan en 1980 « *America is back* ». Certains des principes fondateurs en sont, d'une part, l'opposition aux accords et traités internationaux qui peuvent limiter la souveraineté américaine et, d'autre part, la restriction des interventions militaires aux seules confrontations à une menace directe sur les intérêts nationaux. Cette stratégie doit pouvoir s'appuyer sur un outil militaire robuste capable de dissuader ou de vaincre tout adversaire de façon unilatérale, ce qu'illustre le slogan de l'administration Trump, également emprunté à Ronald Reagan « *peace through strength* » ⁽¹²⁾.

(11) Les *National Security Strategy* (NSS) sont des documents préparés par le pouvoir exécutif fixant les axes principaux de la stratégie américaine.

(12) David NAKAMURA et Juliet EILPERIN, « Trump to focus on 'peace through strength' over Obama's 'soft power' approach », *The Washington Post*, 29 December 2016 (www.washingtonpost.com/).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

L'Otan, une alliance « périssable » ?

« *We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow* »⁽¹³⁾ : prononcés en 1848 par Lord Palmerston (Premier ministre britannique de 1855 à 1858 et de 1859 à 1865), ces mots trouvent un écho particulier dans le contexte actuel où l'Otan s'est vu affublée du qualificatif d'« obsolète » par Donald Trump lors de la campagne électorale. Si, une fois élu, il a tenu à réitérer son attachement à l'Alliance, il n'en demeure pas moins qu'une telle déclaration sonne comme un avertissement à l'oreille de certains alliés dont la sécurité repose en grande partie sur une organisation qu'ils croyaient « éternelle ». Au-delà de cette critique, l'approche transactionnelle de la défense collective mise en avant par Donald Trump, lequel mettait notamment en balance l'effort de défense des alliés européens et la contribution américaine à la défense collective, marque une profonde rupture dans le caractère jusqu'alors inconditionnel de l'engagement des États-Unis dans la défense de l'Europe. Même dans les périodes les plus tendues de la relation transatlantique, comme en 2003 à l'occasion de l'intervention américaine en Irak, cette « inconditionnalité » n'avait été remise en cause. Certains observateurs qualifient cette déclaration, certes électorale, de véritable « révolution copernicienne »⁽¹⁴⁾ dans la mesure où elle traduit le caractère « périssable » d'une Alliance dont le concept même s'était opposé dès l'origine à l'avertissement formulé par Georges Washington dans son discours d'investiture en 1796 à ses compatriotes, les enjoignant de ne pas « lier [leur] paix et [leur] prospérité aux ambitions européennes »⁽¹⁵⁾.

Au-delà de la question de la réalité de la mise en œuvre de ces déclarations, lesquelles ont d'ailleurs été ultérieurement atténuées, se pose le problème de leur perception par les États européens. À cet égard, la réaction de la chancelière allemande Angela Merkel est éclairante sur l'évolution de la vision du lien transatlantique : « Je pense que nous, les Européens, avons notre destin dans nos propres mains. Je vais continuer de m'engager pour que les 27 États-membres travaillent ensemble vers l'avenir (...) face aux défis du XXI^e siècle »⁽¹⁶⁾.

La prise de conscience du caractère non intangible de la protection américaine joue ici un rôle clé dans le processus de développement d'une future défense européenne autonome.

Le « reset » des relations américano-russes et la place de l'Europe dans le système des intérêts stratégiques des États-Unis

L'engagement militaire américain en Europe pose la question de l'évolution de la place de l'Europe dans le système d'intérêts des États-Unis. Dans la stratégie mise en

(13) Martin MURPHY, « The Importance of Alliances for US Security », *2017 Index of US Military Strength*, The Heritage Foundation, 2017, p. 17

(http://ims-2017.s3.amazonaws.com/2017_Index_of_Military_Strength_ESSAYS_MURPHY.pdf).

(14) François HEISBOURG, entretien, 7 février 2017.

(15) Carl C. HODGE et Cathal J. NOLAN, *US Presidents and Foreign policies, From 1789 to the present*, ABC-CLIO, Inc., 2007, p. 388.

(16) « Les Européens ont leur destin "en main", répond Angela Merkel à Donald Trump », *Le Monde.fr*, 16 janvier 2017 (www.lemonde.fr/).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

avant par Barack Obama, le rééquilibrage des forces armées américaines vers la région Asie-Pacifique faisait le postulat d'une Europe stable où l'attitude de la Russie ouvrirait la voie à un apaisement des relations américano-russes. En parallèle, les Européens étaient encouragés à accroître leurs dépenses en matière de défense, renforçant ainsi leur capacité à combattre aux côtés des États-Unis tout en assumant une part plus importante de la défense collective en Europe. Cette stratégie permettait aux États-Unis de disposer des appuis et des marges de manœuvre nécessaires en Europe pour concentrer leurs efforts sur le véritable défi posé à l'hégémonie mondiale américaine : la Chine. Ce désengagement relatif d'Europe ne signifiait toutefois pas que les États-Unis abandonnaient leur *leadership* ni, de fait, leur influence en Europe, particulièrement auprès des alliés du flanc Est, conscients des faiblesses qui perduraient au sein de l'Alliance. Dans ce contexte, l'Europe deviendrait une « masse de manœuvre » pour les forces armées américaines plus qu'un « centre de gravité ».

Outre l'effet potentiellement déstabilisateur sur certains alliés du flanc Est, cette stratégie présente un risque important de voir la Russie profiter de cette situation pour étendre son influence et affaiblir davantage une Europe déjà fragilisée, sans pour autant apporter aux États-Unis l'appui escompté face à la Chine. Une telle perception de l'évolution de la stratégie américaine, dans un contexte de profonde incertitude, ne peut que contribuer à la prise de conscience de la nécessité pour les États européens de prendre en main leur destin.

Contexte d'un désengagement américain d'Europe et scénarios envisageables

Une défense européenne au point mort

Malgré les tentatives successives de relance par la France d'une politique commune de l'Europe en matière de sécurité et de défense, celle-ci peine à se développer. L'Union européenne se cantonne aux quelques missions d'assistance militaire et de maintien de la paix sans qu'une vision commune ambitieuse dans ce domaine ne se dégage véritablement. Un embryon de stratégie semble toutefois se dessiner, sous l'impulsion conjointe de M^{me} Mogherini, Haute Représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité et de Jean-Claude Juncker, président de la Commission européenne. La stratégie globale adoptée en juin 2016⁽¹⁷⁾ et le plan d'actions pour la défense de la Commission européenne en fixent certains contours en reconnaissant notamment l'impératif d'autonomie stratégique, sans pour autant présenter une vision commune ambitieuse à long terme qui serait fondée sur une définition des intérêts communs européens.

La question de fond en matière d'opérations demeure celle de la volonté politique des États de l'UE qui, contrairement à l'Otan, ne dispose pas de *leader* incontesté, à même de fédérer les volontés. On peut noter à cet égard que le *leadership* français sur les questions de sécurité et de défense au sein de l'UE est souvent perçu

(17) *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, juin 2016 (http://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_review_web.pdf).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

comme suspect aux yeux de certains pays européens. De fait, en matière de sécurité et de défense, il n'existe pas, pour l'heure, d'alternative européenne crédible à l'Otan.

Une cohésion occidentale fragilisée

Le *Brexit* fait entrer l'Europe dans une zone de turbulences dont les effets sur la cohésion des différents membres et l'étendue des potentiels dommages collatéraux ne sont pas encore totalement identifiés. Ils seront, pour beaucoup, liés à la nature des négociations et à l'accord éventuel qui en résultera. Si la volonté britannique de préserver le Traité de Lancaster House est aujourd'hui mise en avant, sa pérennité n'est toutefois pas acquise. À l'issue de la sortie du Royaume-Uni de l'UE, la France y sera la seule puissance nucléaire et le seul pays de l'UE à siéger comme membre permanent du Conseil de sécurité des Nations unies ; deux singularités qui risquent d'isoler davantage la France sur le champ de la défense et de la sécurité en Europe.

Le comportement actuel de la Russie est à la fois un facteur exogène d'évolution des organisations, particulièrement de l'Otan dont le volet « défense collective » se trouve réaffirmé mais aussi de désaccords entre pays européens dont les perceptions varient du « risque » à la « menace » russe ce qui impacte les priorités en matière d'allocation de ressources souvent limitées. La montée en puissance de la présence militaire des alliés sur le flanc Est représente, notamment pour la France, une sollicitation supplémentaire, dans un contexte de surengagement de ses forces armées au Sahel, au Levant et sur le territoire national.

Malgré un rôle réaffirmé face au retour de la puissance russe sous l'impulsion conjointe des pays de l'Europe de l'Est et des États-Unis, la cohésion de l'Otan reste fragilisée. Le récent rapprochement de la Turquie et de la Russie, dans un contexte de durcissement du régime de Recep Erdogan éloigné des valeurs prônées par les pays membres de l'Otan et de l'UE, les déclarations du nouveau Président américain et l'affermissement des positions de certains pays du flanc Est, notamment de la Pologne, ouvrent la voie à une potentielle tétanie décisionnelle de l'Alliance. La conséquence pourrait en être une organisation certes « capable », car disposant de capacités militaires et de structures de commandement pertinentes, mais finalement « inutile » car privée de l'expression de la volonté politique des alliés lui permettant d'agir.

L'Otan face aux défis sécuritaires en Europe : les limites du parapluie américain

Les différents pays européens ont majoritairement fait le choix de l'Otan pour garantir la défense de l'Europe : « *NATO, the cornerstone of the West's defence* », comme le rappelait le Premier ministre britannique, Theresa May, devant les membres républicains du Congrès lors de son déplacement à Washington en janvier 2017⁽¹⁸⁾. Selon les pays, cette réalité recouvre différentes stratégies ou intérêts nationaux qui se fondent toutes sur la garantie du parapluie américain, à l'origine de l'Alliance et qui demeure sa principale raison d'être.

(18) [L'Otan, la pierre angulaire de la défense de l'Ouest]. Le texte complet de l'intervention de Theresa May est disponible sur le site www.conservativehome.com.

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

À l'exception de la France et dans une moindre mesure du Royaume-Uni, aucun de ces alliés ne dispose – ni ne cherche véritablement à acquérir – une autonomie stratégique. Pour certains pays comme pour l'Allemagne, celle-ci revêt même un caractère négatif car synonyme d'unilatéralisme. Cette dépendance vis-à-vis des États-Unis offre un certain confort à ces pays au sein de l'Alliance, ce que critique justement le président Trump.

La menace terroriste sur le sol européen, particulièrement en France et en Allemagne, la crise migratoire, la montée en puissance de l'influence chinoise construisant « ses nouvelles routes de la soie »⁽¹⁹⁾ aux portes de l'Europe, sont autant de défis pour la sécurité en Europe et la préservation des intérêts des États de l'UE que l'Otan n'est pas en mesure de relever seule. Les menaces actuelles requièrent en effet une capacité à agir de façon coordonnée sur l'ensemble du continuum sécurité-défense, se traduisant par la mise en œuvre d'une gamme complète d'instruments, non circonscrits au seul domaine de la défense, comprenant notamment la diplomatie, l'économie, la justice, la police dont l'Otan n'est pas dotée.

La prise de conscience de telles limites du parapluie américain au sein de l'Alliance pourrait convaincre certains alliés de faire le choix, à terme, d'une Europe stratégiquement autonome. Toutefois et à court terme, la fragilité de la cohésion des membres de l'Alliance combinée à un rapide désengagement américain pourrait avoir des conséquences particulièrement néfastes sur la sécurité et la défense d'une Europe incapable, pour l'heure, d'offrir une alternative crédible à l'Otan.

Les scénarios d'un désengagement militaire américain d'Europe

Quoique très probable à court terme, le scénario de *statu quo* de l'engagement américain a volontairement été écarté de cette étude car ne constituant pas un déterminant de l'évolution du comportement des pays européens.

Le scénario le plus délétère serait une sortie des États-Unis de l'Alliance dont elle est le principal pilier. Malgré la solidité que lui confère son haut degré d'institutionnalisation, ses processus décisionnels élaborés et sa bureaucratie structurante, ayant notamment contribué à sa pérennité, le choc constitué par le départ de son principal allié et fondateur lui serait d'autant plus fatal que sa cohésion est aujourd'hui fragilisée par des divergences d'intérêts et de perception des menaces associées.

Un tel scénario de retrait des États-Unis de l'Otan, un temps redouté, ne semble toutefois pas probable à court terme. Comme le rappelait récemment Jean-Pierre Maulny, directeur adjoint de l'Iris : « L'Otan est un instrument d'influence irremplaçable des États-Unis sur les Européens, y compris pour y exporter les équipements militaires fabriqués par l'industrie d'armement américaine »⁽²⁰⁾.

(19) Cyrille PLUYETTE, « Les “nouvelles routes de la soie” au cœur de la stratégie de Pékin », *Le Figaro.fr*, 18 janvier 2017.

(20) Jean-Pierre MAULNY, « L'élection de Trump : une impulsion décisive pour l'Europe de la défense ? », novembre 2016 (www.iris-france.org/83497-lelection-de-trump-une-impulsion-decisive-pour-leurope-de-la-defense/).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ? Quelles conséquences stratégiques pour la défense européenne ?

Le scénario intermédiaire consiste en une nette diminution de la présence militaire en Europe associée à un recul partiel du *leadership* américain au sein de l'Otan, sans évolution notable de l'organisation. Deux attitudes opposées des pays européens sont envisageables : un renforcement du comportement de « supplétif » afin de limiter cette érosion du parapluie américain en évitant par tous les moyens d'apparaître comme autonome aux yeux des États-Unis ou, au contraire, un renforcement du pilier européen de l'Alliance sous l'impulsion conjointe d'une prise de conscience du caractère inexorable du désengagement américain d'Europe et de l'affirmation d'un *leadership* coordonné des principaux alliés européens.

On peut en outre concevoir une présence militaire permanente en Europe limitée aux seuls points d'appui sur lesquels seraient prépositionnés un certain nombre d'équipements, permettant un déploiement rapide de forces en cas de montée en puissance d'une menace. Cette option s'inscrit dans la droite ligne des mesures de « présence avancée renforcée » en cours d'implémentation en Europe centrale et orientale. Ce scénario peut être combiné au précédent, venant ainsi atténuer la perception d'abandon des pays européens, ce qui aurait pour effet potentiel de limiter l'ampleur de la réaction soit de « supplétif », soit d'affirmation du *leadership* européen.

Quel que soit le scénario envisagé, y compris celui de *statu quo*, l'évolution des menaces et de leur perception par les pays européens, particulièrement sur le flanc Est, aura une incidence forte sur la relation transatlantique.

Conséquences stratégiques pour la France et l'Europe

La France comme pivot de la construction d'une défense européenne

Il convient d'aborder cette réflexion sur le désengagement militaire américain dans une dimension géographique plus large englobant la sphère des intérêts des pays européens (Arctique, Balkans, Proche et Moyen-Orient, Afrique du Nord...). Certains signes de ce désengagement sont, à cet égard, déjà perceptibles : intervention en Libye, frappes en Syrie, sont autant d'illustrations de l'effacement relatif du *leadership* américain dont l'un des effets notables est une implication militaire croissante de la France sur la scène internationale. Cette attitude française, que l'on peut qualifier d'« interventionniste », tire en outre parti de la doctrine américaine de « *leading from behind* », la France bénéficiant de l'appui de capacités clés pour ses opérations, souvent en nombre insuffisant dans les forces armées françaises (drones, avions ravitailleurs), et d'une coopération accrue entre forces spéciales françaises et américaines.

Dans ce cadre, la démonstration de la puissance militaire française, combinaison de l'affirmation d'une volonté politique et de la cohérence d'un outil de défense bénéficiant d'une épaisseur opérationnelle avérée, confère une crédibilité renforcée à la France dans le rôle de pivot qu'elle est amenée à jouer dans le développement d'une défense européenne. Dans la perspective d'un effacement partiel du parapluie américain, la dimension nucléaire des forces armées françaises peut être un atout supplémentaire que le départ de la Grande-Bretagne de l'UE ne fait qu'exacerber. Si cette dissuasion

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

nucléaire est aujourd'hui strictement nationale, à terme, se poseront toutefois les questions de la place de cette dissuasion et de son poids relatif dans la défense de l'Europe.

L'axe franco-allemand : maintenant ou jamais

Depuis la fin de la Seconde Guerre mondiale, la France s'est attachée à ancrer l'Allemagne au sein d'institutions européenne et atlantique robustes. Comme l'écrit Frédéric Bozo ⁽²¹⁾ : « Le partenariat franco-allemand est aujourd'hui plus vital que jamais afin d'orienter le rôle de l'Allemagne et d'assurer son engagement durable envers le projet européen et l'alliance transatlantique à un moment où les deux pays sont testés comme jamais auparavant. Dans le contexte de la crise de l'Euro, toujours en cours, des inquiétudes croissantes à propos de l'avenir de l'ordre libéral occidental et international, dans le sillage du vote du *Brexit* et de l'élection de Donald Trump, et tandis que des élections majeures auront lieu dans ces deux pays en 2017, le partenariat franco-allemand importe beaucoup pour l'avenir de l'Europe et de l'Occident. »

Malgré des divergences plus ou moins marquées, la qualité de la relation entre la France et l'Allemagne a joué et continue de jouer un rôle clé dans le processus de construction européenne. Ainsi, ces deux pays sont à l'origine de la Communauté européenne et ont, par la suite, réussi à absorber le choc de la réunification. En 2003, c'est « épaulement contre épaulement » qu'ils se sont opposés à l'intervention américaine en Irak puis ont mis tout en œuvre, l'année suivante, pour normaliser la relation États-Unis–Europe et rétablir la cohésion transatlantique. Récemment encore, dans le cadre de la crise de l'Euro, France et Allemagne ont su dépasser leurs différends pour adopter une position commune, préservant à la fois les intérêts nationaux et ceux de l'Europe.

Par ailleurs, et comme l'a démontré son rôle dans le processus de règlement de la crise russo-ukrainienne aux côtés de la France (Conférence de Minsk), l'Allemagne est aujourd'hui un acteur majeur sur la scène internationale. Ses ambitions en matière de défense s'affirment pas à pas : le *Livre blanc* allemand de 2016 sur « la politique et l'avenir de la *Bundeswehr* », les annonces relatives à l'augmentation du budget de la défense vers 2 % du PIB et son rôle actif en matière de coopération de défense, sont autant de signes de l'émergence d'un partenaire crédible avec lequel la France doit poser les bases d'une coopération européenne multilatérale. Encore faut-il que la France poursuive ses efforts en matière de défense pour ne pas déséquilibrer ce partenariat.

Même si les différences d'architectures institutionnelles d'emploi des forces induisent certains freins dans le développement du partenariat franco-allemand, les conditions existent de part et d'autre des deux rives du Rhin pour l'affirmation d'un couple franco-allemand comme catalyseur de coopérations européennes de sécurité et de défense, ouvert sur des partenaires majeurs de la France tels que l'Italie. Cette voie des coopérations structurées permanentes, permises par le traité de Lisbonne, est d'ailleurs mise en avant dans l'un des scénarios d'évolution de la construction européenne, récemment proposés par Jean-Claude Juncker.

(21) Frédéric BOZO, « Whither Germany ? Why France matters, The German Marshall Fund of the United States », 31 janvier 2017 (www.gmfus.org/publications/whither-germany-why-france-matters).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ? Quelles conséquences stratégiques pour la défense européenne ?

La pertinence de ce moteur franco-allemand repose en outre sur une perspective continentale commune se distinguant en cela du partenariat franco-britannique dont la valeur opérationnelle et technologique doit toutefois être soulignée. Dans cet esprit, les deux partenariats ne doivent pas être considérés comme exclusifs l'un de l'autre.

La BITDE comme socle de la défense européenne

Renforcer la Base industrielle et technologique de défense européenne (BITDE) par une politique européenne volontariste est aujourd'hui une nécessité. Il ne faut toutefois pas encourager une attitude de « forteresse européenne » dans le secteur de l'armement qui n'aurait d'autre effet néfaste que d'attiser les tensions industrielles et commerciales entre les deux rives de l'Atlantique. La mise en œuvre d'une telle politique nécessite toutefois l'acceptation par les États-Unis du caractère stratégique pour l'Europe de la préservation d'une BITDE indissociable de la défense de ses intérêts.

Une telle politique européenne doit en outre permettre de prévenir les effets d'une réaction de « supplétif » de certains alliés européens, liée à la crainte d'un désengagement américain qui consisterait à « acheter » la sécurité américaine par le biais de son industrie de défense, dans une logique transactionnelle, chère au président Trump. Dans un discours sur l'Europe, prononcé le 6 octobre 2016, François Hollande met en garde contre ce comportement de « supplétif » de certains alliés, critiquant ainsi implicitement l'attitude de la Pologne ⁽²²⁾ : « Il y a des pays européens qui pensent que les États-Unis seront toujours là pour les protéger, au point même d'acheter des armes uniquement aux États-Unis et pas aux Européens. Il y a des pays qui pensent qu'il y aura toujours une couverture qui viendra les mettre à l'abri de toutes les influences. »

La perception d'un désengagement inexorable des États-Unis des affaires européennes, couplée à la prise de conscience des limites du parapluie américain face aux défis sécuritaires, auxquels l'Europe est confrontée, peut créer les conditions favorables d'une coopération interétatique accrue. S'appuyant sur des convergences industrielles éprouvées, à l'instar de groupes MBDA ou Airbus, la stratégie européenne pourrait, notamment, consister en une sectorisation partielle des industries de défense européennes respectant les savoir-faire technologiques et créant les conditions pour l'émergence de « champions européens ».

Otan-UE : vers une complémentarité assumée

Le cadre sécuritaire actuel où se combinent le retour des États puissance et le terrorisme islamiste, met en évidence la complémentarité et le renfort mutuel théorique entre l'Otan et l'UE. Cette dernière permet en effet une approche globale des questions de sécurité et de défense, forte de la variété des instruments politiques et des moyens militaires qu'elle peut combiner, tandis que l'Otan, s'appuyant sur la puissance militaire américaine, est naturellement plus apte que l'UE aux opérations dites du « haut du spectre ».

(22) « Achat d'hélicoptères : la Pologne délaisse la France pour les États-Unis », *Le Monde.fr*, 11 octobre 2016 (www.lemonde.fr/).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

Une complémentarité assumée entre ces deux entités doit permettre, en outre, d'ouvrir la voie à l'émergence à terme d'un pilier européen au sein d'une Alliance réaffirmée dans son rôle central de défense de l'Europe et de préservation du lien transatlantique. Un tel pilier ne pourra toutefois émerger que si les alliés européens assument pleinement leurs responsabilités en matière de défense au sein des deux organisations ce qu'illustrent les propos du Sénateur américain, William Roth ⁽²³⁾ : « Les États-Unis doivent faire tout leur possible pour encourager la consolidation des efforts européens dans le domaine de la défense. Mais ils ne doivent pas être tenus pour responsables de l'incapacité des États européens de jouer un rôle plus cohérent au sein de l'Alliance. Il incombe aux Alliés européens de développer des capacités européennes de sécurité et de défense pour donner une véritable signification à l'identité européenne de sécurité et de défense. »

L'objectif est bien de renforcer la complémentarité entre l'Otan et l'UE dans une démarche « gagnant-gagnant » qui, comme l'encourage François Heisbourg ⁽²⁴⁾, doit dépasser la rhétorique négative des « trois D » qui synthétise les risques de « découplage », de « duplication » et de « discrimination » couramment opposés au développement de la politique commune de sécurité et de défense. À cet égard, une étape encourageante a été franchie, à l'occasion du Sommet de Varsovie en 2016, où la complémentarité des deux organisations a été réaffirmée au travers d'une déclaration conjointe Otan-UE ⁽²⁵⁾.

Conclusion

En s'appuyant sur un lien historique renouvelé, ce n'est que dans une relation transatlantique équilibrée qu'une défense européenne pourra émerger.

Les déclarations du Président américain nouvellement élu, son tropisme nationaliste, son approche transactionnelle des relations interétatiques, combinés aux défis du terrorisme islamiste et de la crise migratoire en Europe constituent autant d'occasions pour les pays européens de prendre conscience de la nécessité d'assumer leur propre défense. Dans ce contexte, le désengagement militaire américain d'Europe est avant tout affaire de perception : celle de la place de l'Europe dans le nouveau système des intérêts américains. La stratégie du rééquilibrage vers la région Asie-Pacifique, que le déploiement d'unités américaines en Europe centrale et orientale aurait pu faire oublier, reste une tendance de fond de la stratégie globale américaine depuis les « années George W. Bush ».

La France, seul État de l'UE à disposer d'une autonomie stratégique, fondée sur une dissuasion nucléaire crédible, doit saisir cette opportunité pour jouer un rôle pivot dans la construction d'une défense européenne revitalisée. Portée par un partenariat

(23) William V. ROTH JR., *Nato in the 21st Century*, septembre 1998, p. 57.

(24) François HEISBOURG, « La défense européenne fait un bond en avant », *Revue de l'Otan*, Printemps-Été 2000, vol. 48 (www.cvce.eu/).

(25) Déclaration sur la mise en œuvre des dispositions de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Otan, nato.int, 6 décembre 2016 (www.nato.int/cps/fr/natohq/official_texts_138829.htm).

Désengagement militaire américain d'Europe : trompe-l'œil ou réalité ?
Quelles conséquences stratégiques pour la défense européenne ?

franco-allemand plus ambitieux et ouverte sur un ensemble de coopérations entre États européens, incluant en particulier l'Italie, cette défense devra intégrer la Grande-Bretagne et s'appuyer sur une BITDE soutenue par une politique européenne volontariste.

L'émergence d'une défense européenne structurée, bénéficiant à terme d'une autonomie stratégique, et dont les États-membres assument par ailleurs pleinement leurs responsabilités au sein de l'Alliance, doit être perçue comme un atout pour notre allié américain et non comme une menace sur ses intérêts, répondant ainsi aux vœux formulés par Henri Kissinger en 1973 ⁽²⁶⁾ : « Tout comme l'autonomie de l'Europe n'est pas une fin en soi, de même la Communauté européenne ne peut être un club exclusif (...). Nous espérons que nos amis européens se joindront à nous dans cet esprit. »

Éléments de bibliographie

Ouvrages

- The Military Balance 1989-1990*, Brassey's, International Institute for Strategic Studies, octobre 1989.
- The Military Balance 1999-2000*, Oxford University Press, International Institute for Strategic Studies, octobre 1999.
- The Military Balance 2008*, Pub. Routledge, International Institute for Strategic Studies, février 2008.
- The Military Balance 2010, The Annual Assessment of Global Military Capabilities and Defence Economics*, Routledge for the International Institute for Strategic Studies, février 2010.
- The Military Balance 2016, The Annual Assessment of Global Military Capabilities and Defence Economics*, Routledge for the International Institute for Strategic Studies, février 2016.
- The Military Balance 2017, The Annual Assessment of Global Military Capabilities and Defence Economics*, Routledge for the International Institute for Strategic Studies, février 2017.
- KASHMERI Sarwar A., *NATO 2.0 Reboot or Delete?*, Washington DC, Potomac Books Inc., 2011 ; 280 pages.
- KEMPF Olivier, *L'Otan au XXI^e siècle, La transformation d'un héritage*, Éditions du Rocher, 2014 ; 614 pages.
- OSWALD Franz, *Europe and the United States, The Emerging Security Partnership*, Praeger Security International Publishers, 2006 ; 200 pages.
- TERCINET Josiane (dir.), *Les relations transatlantiques et l'environnement international*, Bruxelles, Bruylant, 2005 ; 262 pages.
- PETERSSON Magnus, *The US NATO Debate: From Libya to Ukraine*, New York, Bloomsbury, 2015 ; 224 pages.
- BOZO Frédéric, *Histoire secrète de la crise irakienne, La France, Les États-Unis et l'Irak 1991-2003*, Perrin, 2013 ; 408 pages.

Liste des entretiens (par ordre alphabétique)

- BOZO Frédéric (Professeur, Université Sorbonne Nouvelle – Paris 3).
- Brustlein Corentin (Chercheur, Responsable du Centre des études de sécurité de l'Institut français des relations internationales et du programme « Dissuasion et prolifération »).
- GONDALLIER DE TUGNY Didier (Conseiller chargé des affaires UE-Otan et des relations institutionnelles françaises, MBDA).
- HEISBOURG François (Conseiller spécial du président de la Fondation pour la recherche stratégique, FRS).
- RAZOUX Pierre (Directeur de recherches à l'Institut de recherche stratégique de l'École militaire, Irsem).

(26) Henri KISSINGER, Discours, New-York, 23 avril 1973
(www.cvce.eu/content/publication/2002/9/30/dec472e3-9dff-4c06-ad8d-d3fab7e139f/publishable_fr.pdf).

Les possibles évolutions de la relation franco-britannique d'ici dix ans

Robert J. THOMSON

Général de brigade, *CBE* (Ordre de l'Empire britannique)
DSO (Ordre du service distingué). Auditeur de la 66^e session du Chem.

Lorsqu'on se trouve dans l'élégante bibliothèque au sein de la résidence de l'ambassadeur britannique à Paris, on ressent clairement le contexte historique des relations de défense et de sécurité nationale entre le Royaume-Uni et la France. C'est ici que, après la Libération de Paris, Duff Cooper, le premier ambassadeur britannique après la Seconde Guerre mondiale, a travaillé très tard chaque nuit afin d'initier un premier traité de défense entre les deux Nations : le Traité de Dunkerque sera signé en 1945.

D'une manière curieuse, cette fois, c'est le Royaume-Uni qui a été le partenaire le plus hésitant. En dépit de sa lutte contre le nazisme avec les Forces françaises libres, l'armée de terre britannique a dit qu'elle n'était pas prête à reprendre les réunions officielles entre les deux armées ! Pourtant, 72 ans plus tard, les relations franco-britanniques sont encore plus importantes dans un monde où l'ordre international est menacé. En outre, la nature de ces menaces qui vont à l'encontre de la stabilité, tant à l'intérieur qu'à l'extérieur de nos pays, évolue constamment. L'imprévisibilité caractérise cette ère qui a fondamentalement changé et c'est cette imprévisibilité, qui se trouve au cœur de tant de menaces contemporaines, qui est l'élément le plus inquiétant dans l'environnement politico-militaire actuel. Il semble que cette imprévisibilité dominera de plus en plus le contexte stratégique moderne dans les dix prochaines années. À certains égards, 2017 est une année pivot, qui suit les surprises stratégiques du *Brexit* et de la présidentielle américaine de 2016. C'est l'année durant laquelle les conséquences d'un retrait américain du *leadership* du monde occidental seront visibles. Pour l'Europe, les scrutins néerlandais, français, allemands et potentiellement italiens vont façonner le paysage politique de la décennie à venir, y compris le fond et la forme des négociations sur le *Brexit*.

Pour faire face à l'imprévisibilité, la tendance forte cultivée par les États est de se raccrocher à la certitude qu'ils pourront renforcer leur sécurité grâce à leurs alliés et à des alliances éprouvées et respectées. Celles-ci reposent sur un rapport établi dans une histoire partagée, sur des valeurs communes. Mais, au-delà, dans un monde de plus en plus orienté sur lui-même, sur un intérêt national plus que jamais dimensionnant,

ce sont ces intérêts nationaux qui constitueront le socle de cette relation bilatérale dans la décennie à venir. Les deux Nations ont eu des rapports historiquement compliqués mais ce n'est pas l'objet de cette étude. Ce qui est évident, c'est le fait que la France et le Royaume-Uni partagent une vision commune, qui, trop souvent, est sous-estimée. Tous deux sont des puissances nucléaires et occupent un siège permanent au Conseil de sécurité à l'ONU. Tous deux ont des ambitions commerciales globales et voudraient que les valeurs et les principes de la démocratie, du marché libre et des droits de l'homme, puissent être préservés à travers le monde. Tous deux ont gardé une capacité militaire expéditionnaire sur tout le spectre et ont d'ailleurs prouvé qu'ils restent en mesure de déployer une force militaire capable de protéger leurs intérêts, à l'intérieur ou à l'extérieur du pays, d'une manière indépendante ou bilatérale. Leur capacité économique est comparable, même si les systèmes sont assez différents. Par leur héritage colonial, les deux pays gèrent leur propre réseau mondial.

Mais ces amitiés ne sont jamais garanties. Certes, les conditions de base pour des relations proches et pour la coopération dans le domaine de la défense et de la sécurité nationale sont en place. Pourtant rien n'est jamais acquis. Toute relation a besoin d'attention et de soin pour en assurer la survie. Cette étude examinera d'abord le contexte des relations franco-britanniques dans les dix années à venir et comment ce contexte international pourrait faire évoluer ces relations au niveau politico-militaire. Par la suite, les « *game-changers* » potentiels, qui pourraient menacer ce rapport seront examinés. Enfin, il sera proposé quelques domaines dans lesquels la France et le Royaume-Uni pourraient approfondir leur relation.

Lancaster House : actuellement et dans les années à venir

Selon la *Strategic Defence and Security Review* de 2010, la première revue britannique qui a traité de sécurité nationale en général et pas uniquement de l'enjeu de défense, les Britanniques ont constaté que la France était un de ses principaux alliés stratégiques, juste après les États-Unis. Et, la même année, le 2 novembre, le Traité de Lancaster House a été signé par le Premier ministre Cameron et le président Sarkozy. En 2011, les deux pays organisaient des opérations, interarmées et interalliées, en Libye. Les trois éléments (le développement conjoint de capacités, la coopération nucléaire, et la naissance d'une force interalliée et expéditionnaire) se renforcent mutuellement. Néanmoins, c'est l'élément nucléaire qui garantit que le Traité ne sera jamais élargi à d'autres pays européens. Ce qui fait la force de ce Traité, c'est son bilatéralisme et la parité des deux pays participants. Il n'y a aucun signe que le Traité se voit élargi ou abandonné mais il faut y porter une attention constante pour assurer que les progrès nécessaires sont accomplis et que le niveau d'ambition reste assuré. Les processus qui soutiennent ce Traité ont déjà été mis en œuvre et Lancaster House, souvent cité, se fonde sur une exigence de coopération. Cet impératif a transformé les relations dans certains domaines : par exemple, le rapport entre les deux armées de terre n'a jamais été aussi proche et pour chaque exercice les deux brigades nationales d'entrée en premier accueillent leur binôme. Le rythme bisannuel des sommets franco-britanniques (2010, 2012, 2014 et 2016) garantit le soutien direct du Président et du Premier ministre, qui restera important dans cette décennie, étant donné que le Traité

est, à l'origine, le travail de leurs prédécesseurs. Les trois composantes restent importantes et dureront au moins jusqu'en 2027, avec la composante nucléaire comme socle de l'édifice.

Le contexte

Le monde reste un endroit incertain et les menaces à l'ordre international sont palpables. La Russie présente un défi jamais connu depuis 1989, et il semble qu'elle ne tienne pas compte volontairement des frontières internationales. Il n'est pas évident, non plus, de savoir quand la crise au Moyen-Orient prendra fin. Les situations en Irak et dans les pays ayant connu des Printemps arabes et l'action de *Daesh* restent confuses et complexes. Il semble que l'Afrique, de plus en plus, se désintègre. Il y a, également, une rivalité entre les principales puissances du Pacifique. En outre, la menace terroriste peut changer les priorités politiques à court terme, au niveau national ou international, au détriment des priorités de moyen terme et long terme. Cette étude n'examinera pas ces menaces, bien qu'elles encadrent d'une manière significative le contexte, présent ou émergent, de la relation franco-britannique, mais elle examinera trois influences qui encadrent cette relation : le *Brexit*, la présidentielle américaine et la recherche d'une identité de défense européenne ⁽¹⁾.

Le Brexit

Le *Brexit* va dominer les gros titres politiques pendant la première partie de la décennie qui arrive, voire la décennie entière. Une transformation radicale dans le rapport économique avec les pays restant dans l'UE en découlera qui, selon notre Premier ministre ⁽²⁾, donnera au gouvernement la capacité d'établir ses propres règlements et de construire des accords commerciaux nouveaux et dynamiques, dans les intérêts du Royaume-Uni. Alors que le Premier ministre ne cite pas la défense dans ses 12 objectifs pour les négociations ⁽³⁾, elle cite la coopération dans la lutte contre le crime et contre le terrorisme ⁽⁴⁾. L'intention explicite de la part des militaires est bien de protéger les relations de défense, quel que soit le type des négociations qui entourent la sortie britannique de l'UE. Les deux Chefs d'état-major des armées (Céma) ont insisté sur ce point lors de réunions publiques. Cette intention est partagée des deux côtés de la Manche. Le Royaume-Uni peut et devrait démontrer sa crédibilité européenne dans le monde de la défense et de la sécurité nationale. En même temps, toute tentative d'utiliser le surplus sécuritaire britannique dans les négociations devrait être évitée. Les effets sur les relations de défense seront négatifs et nuiront à la confiance mutuelle. Le Royaume-Uni voudra, peut-être, augmenter ses équipes d'attachés de défense dans les ambassades européennes pour mieux comprendre les postures nationales de chaque pays et les enjeux de la défense européenne. Certaines rumeurs ont été entendues, y compris à Paris, que le Royaume-Uni devrait transférer le poste de *DSACEUR*

(1) Il ne sera pas traité les risques sur l'unité du Royaume-Uni, qui influencerait grandement les relations de défense.

(2) Malcolm CHALMERS, « UK Foreign and Security Policy after Brexit », *RUSI Briefing Paper*, janvier 2017, p. 2.

(3) Theresa MAY, « PM Speech to the Lord Mayors Banquet », Guildhall, Londres, 14 novembre 2016.

(4) Objective 11. « Co-operation in the fight against crime and terrorism. We will continue to work closely with our European allies in foreign and defence policy even as we leave the EU itself. »

(Commandant adjoint des opérations de l'Otan), britannique depuis 1951, à un autre pays encore membre de l'UE : cela souligne la difficulté, au moins aux yeux européens, de protéger la position du Royaume-Uni à l'Otan suite au *Brexit* ⁽⁵⁾.

Il y a potentiellement 4 risques qui, probablement, affecteront le Royaume-Uni plus que l'Europe, mais pourront néanmoins affaiblir la réponse européenne en général face aux crises. Le premier est simplement une question volumétrique : gérer le *Brexit*, avec toute sa complexité et sa sensibilité politique, présente un défi important pour le gouvernement britannique chez lui, dans les missions auprès des organisations internationales et dans les ambassades à travers le monde. Il faut que la question soit posée sur la capacité et sur la volonté britannique de gérer d'autres enjeux au-delà du *Brexit* lui-même. Comme Malcolm Chalmers le signale ⁽⁶⁾, le risque est réel de voir les politiques de défense et des affaires étrangères négligées du fait que le gouvernement utilise sa capacité limitée pour prioriser les enjeux les plus proches. Le deuxième risque demeure que l'accord commercial négocié, concomitant au *Brexit*, complique d'une manière financière et commerciale la coopération qui a été bien établie dans le monde des armements. Il est possible qu'il y ait un élément subordonné à ce risque qui pourrait augmenter la tension entre la rhétorique française sur l'autonomie stratégique de l'UE, en particulier dans le domaine des capacités, et l'importance de la coordination franco-britannique sur les armements. Le troisième risque est que le rôle traditionnel de pont diplomatique entre les États-Unis et l'Europe devienne beaucoup plus compliqué en même temps que les menaces sur le voisinage européen augmentent. En outre, subsistera une tension entre l'ambition du Premier ministre pour un Royaume-Uni global et le besoin, dans cette ère de menaces élevées, de renforcer l'identité de défense européenne. Enfin, le quatrième risque pour la relation avec la France, est qu'un agenda britannique de plus en plus nationaliste au sein de la politique sécuritaire pourrait faire diverger les intérêts nationaux et réduire l'impératif de coopérer dans le domaine de la sécurité. *In fine*, le coup de main que les Britanniques doivent donner est d'équilibrer une volonté d'approfondir leur influence globale avec un intérêt de sécurité et de stabilité européenne durable.

Le président Trump

Deuxièmement, l'élection du président Trump et les conséquences pour les relations franco-britanniques. C'est l'imprévisibilité qui émerge autour de cette présidence et qui est sans précédent. La nature réactionnaire de ses décisions pourrait également menacer les relations franco-britanniques mais, à certains égards, rendre aussi les relations bilatérales encore plus solides dans les dix années à venir. Ses critiques incessantes et publiques de ses propres organisations de renseignements constituent un bon exemple organique de son imprévisibilité mais c'est son scepticisme sur les institutions multilatérales et internationales qui présente le défi le plus important face à l'édifice moderne international. Le Royaume-Uni et la France devront être préparés à une relation beaucoup plus transactionnelle. Il faudra que tous deux comblent l'écart

(5) Malcolm CHALMERS, « UK Foreign and Security Policy after Brexit », p. 1.

(6) Malcolm CHALMERS, *op. cit.*, p. 3.

intellectuel entre les États-Unis et l'Europe, en maintenant le président Trump au sein de l'Otan et, en même temps, en poussant l'Europe vers M. Trump, malgré sa rhétorique (« *America first* ») et en le soutenant, par exemple, lorsqu'il exige que les pays européens augmentent leurs dépenses de défense pour l'Otan. La France et le Royaume-Uni doivent ouvrir la voie. Le succès du Premier ministre britannique d'obtenir une affirmation publique de M. Trump était important et, montre, semble-t-il, que l'effort pour préserver la relation transatlantique va augmenter dans la décennie à venir. Le monde a déjà vécu des ères de désengagement américain qui ne se sont jamais bien terminées. Bien que M. Trump ait soixante-dix ans, il est vraisemblable qu'il ne se satisfasse pas d'une période de quatre ans et donc que sa présidence dans les quatre à huit années à venir encadrera les relations franco-britanniques, tant sur la forme que sur le fond. Ainsi, il revient à la France et au Royaume-Uni de travailler de plus en plus de concert lorsqu'ils se préoccupent des enjeux de défense et de sécurité nationale avec les États-Unis. À court terme, cela dépendra de la relation que M. Trump voudra établir avec l'UE et cette attitude se manifesterà dans son choix concernant l'ambassadeur américain auprès de l'Union européenne. La France et le Royaume-Uni devront bâtir les relations les plus fortes avec ceux qui sont les plus proches du Président, le *Secretary of Defence*, par exemple, afin d'éviter les décalages potentiels. Il y a un risque que le Président américain puisse adopter des relations asymétriques avec le Royaume-Uni et la France, en favorisant l'un ou l'autre, compte tenu de sa méfiance vis-à-vis de l'UE et de sa tendance à privilégier un terrain qui soit culturellement sûr pour lui au niveau personnel.

Il convient que les Britanniques n'acceptent pas une telle perspective qui nuirait à l'Otan et à la relation franco-britannique. En outre, si les États-Unis adoptent une posture beaucoup plus isolationniste, une relation opérative entre la France et le Royaume-Uni, qui est solide et fiable, sera le socle de la défense de l'Europe à long terme.

Une politique commune de sécurité et de défense

Troisièmement, et liée d'une manière intime aux deux thématiques précédentes, la perspective d'une identité de défense européenne au-delà de l'Otan progresse. Il faut que le Royaume-Uni gère sa relation avec l'UE *post-Brexit* dans le domaine des affaires étrangères tout en gardant la prééminence de l'Otan en tant que pierre angulaire de la défense européenne. Bien que l'influence britannique sur l'ordre du jour de la sécurité européenne doive rester considérable en tant que membre de l'Otan volontaire, expéditionnaire et possédant des capacités importantes, le Royaume-Uni devra, néanmoins, être préparé à n'avoir qu'une influence extérieure sur les initiatives de défense européenne. La France, grâce à ses liens proches et déclarés, devrait être un pont vers l'organisation de l'UE.

La défense sera un des domaines où le Royaume-Uni pourra continuer à démontrer ses références européennes, claires et elles aussi déclarées. Mais le Royaume-Uni devrait être réaliste à l'égard du degré de sa participation au processus de prise de décision et devrait penser attentivement à la manière la plus efficace d'influencer la construction européenne à venir. En outre, étant donné que la nature de l'environnement

contemporain opératif évolue, et que les leviers économiques diplomatiques et numériques sont de plus en plus importants, le fait que le Royaume-Uni soit à l'extérieur de l'organisation des prises de décision concernant, par exemple, les sanctions, rendra beaucoup plus difficile et compliquée la mise en œuvre de l'influence britannique. Le Royaume-Uni continuera à soutenir la Politique commune de sécurité et de défense (PCSD), à condition qu'elle ne soit pas un rival de l'Otan concernant les ressources. Toutefois, après le *Brexit*, il pourra influencer de moins en moins la route qui sera prise.

Pivots potentiels 2017-2027

Un certain nombre de facteurs pourraient potentiellement changer la donne des relations franco-britanniques dans les dix années à venir. Les principaux sont présentés ci-après.

Un rapport de plus en plus exclusif avec les États-Unis

Il existe un risque qu'en quittant l'UE, le Royaume-Uni se tourne vers les États-Unis sur les plans politique et sécuritaire, et tourne ainsi le dos à ses alliés européens alors qu'il tente d'établir un « *global Britain* » et que ses alliés européens tentent de construire des mécanismes de défense de plus en plus européens, dans un contexte mondial de repli sur soi. Il est également possible que les États-Unis développent une posture plus isolationniste, forçant le Royaume-Uni à se replier sur lui-même. En conséquence, les relations franco-britanniques pourraient devenir de moins en moins importantes, comme d'ailleurs les relations franco-américaines.

Des gouvernements plus repliés sur eux-mêmes et plus nationalistes

Des scrutins doivent se tenir en France en 2017, 2022 et 2027, alors que le Royaume-Uni se choisira de nouveaux gouvernements en 2020 et 2025. À la lumière des résultats du vote sur le *Brexit* et de la présidentielle américaine, les pronostics seraient prématurés et imprudents, mais il est possible que les mouvements de repli sur soi et populistes dans l'un de ces deux pays (ou les deux) gagnent en ampleur et prennent les rênes du pouvoir avec un dirigeant qui serait prédisposé à mettre un terme aux coopérations bilatérales, et potentiellement multilatérales, ou plus probablement à cesser d'investir dans ces coopérations. Quels que soient les résultats des scrutins à venir, le décalage entre les calendriers électoraux des deux États reste un point de friction qu'il faudra gérer.

Un rapprochement entre la France et la Russie

La résurgence de la Russie est interprétée différemment dans chaque capitale européenne – la différence de perception entre la France et le Royaume-Uni peut être caractérisée comme suit : le Royaume-Uni perçoit la Russie comme une menace et la France la regarde comme un facteur de risque sécuritaire. Deux des candidats à la présidentielle française, M. Fillon et M^{me} Le Pen, ont signalé leur intention de tenter un rapprochement avec la Russie (bien que de façon différente) et toute divergence

significative avec la posture britannique pourrait menacer la coopération de défense. La manière dont le président Trump articulera la politique russe des États-Unis aura un impact fondamental sur cette question.

Un Brexit très difficile

Le débat relatif au *Brexit* bat son plein et le défi consiste à parvenir à une sortie négociée et à un nouvel accord commercial qui préserve largement les intérêts politiques et économiques des deux parties. Le Royaume-Uni est clair sur le fait qu'il souhaite voir une Europe forte au cours des prochaines années. Cependant, un *Brexit* très dur, qui pourrait être caractérisé par un retour aux tarifs douaniers de l'Organisation mondiale du commerce (OMC) et des difficultés dans le règlement de la dette Royaume-Uni–Europe, pourrait affecter la coopération en matière de défense et de sécurité. La France, aux côtés de l'Allemagne, jouera un rôle clé dans les négociations et ressentira donc d'autant plus fortement au niveau national le succès ou l'échec de ces négociations.

Les thématiques de long terme

Il y a trois thématiques qui devraient caractériser la relation durable : reconnaître tout d'abord que les intérêts nationaux dirigeront les relations, ensuite que le rapport de défense devrait être élargi pour inclure les enjeux de sécurité en général et, enfin, l'interopérabilité devrait pousser le développement de capacités et, également, l'architecture opérationnelle. Malgré un contexte complexe et changeant, et potentiellement quelques turbulences sur le chemin, la relation de défense franco-britannique se poursuivra et prendra une ampleur croissante à mesure que le Royaume-Uni s'éloignera de l'UE. Le moteur le plus important pour la poursuite de cette coopération dans les années à venir sera la convergence entre les intérêts nationaux du Royaume-Uni et ceux de la France – protéger le territoire national (sur ce territoire et à l'étranger), protéger la population (sur le territoire national et à l'étranger) et faire en sorte que l'économie globale continue à opérer au bénéfice de la communauté internationale. Bien qu'il existe des différences en termes d'échelle et d'acuité, notamment pour ce qui concerne les défis posés par les migrations et le terrorisme islamiste, les menaces auxquelles le Royaume-Uni et la France doivent faire face les affecteront de manière quasi similaire. Et puisque les politiques de défense et de sécurité sont fondamentalement focalisées sur la protection des intérêts nationaux, il existe des avantages mutuels à la poursuite de la coopération. La raison d'être de cette coopération n'est donc pas remise en cause.

Jusqu'à présent, le Traité de Lancaster House s'est focalisé sur la coopération de défense, bien établi dans un contexte de sécurité nationale. Alors que les menaces évoluent, il y aurait intérêt à élargir cet accord pour prendre en compte celles qui sont apparues, ainsi que les cyberattaques contre les Nations, les institutions et les individus. En 2010, le Royaume-Uni a orienté sa première revue de la défense et de la sécurité autour de ces questions. Puisque les relations au niveau institutionnel entre les services de renseignements, les policiers et les douaniers, britanniques et français, sont

solides, une approche commune des défis sécuritaires pourrait éviter les lignes de fracture dans cette lutte institutionnelle contre les menaces contemporaines.

L'interopérabilité reste la voie la plus importante pour développer la coopération de défense entre les deux pays. Cette interopérabilité se joue aux niveaux conceptuels, physiques et moraux : il s'agit de comprendre comment chaque pays pense en stratégie et comment nos militaires élaborent leurs concepts d'opérations. Se connaître apparaît donc essentiel. Il est également important de coopérer quand les deux pays tirent les leviers diplomatiques, politiques et économiques. Il faut que les systèmes puissent travailler ensemble dans l'ère technologique que nous vivons. Il faut que les deux armées puissent se soutenir pour les actions cinétiques, le recueil de renseignement, le ravitaillement ou la communication, quels que soient les domaines (terrestre, aérien ou maritime). Les défis principaux resteront en général la communication et le partage du renseignement. Il y a également un aspect moral à cette interopérabilité qui, actuellement, a une importance significative dans l'art d'exercer le commandement des opérations stratégiques, opératives ou tactiques. Certaines restrictions sur les sujets juridiques, certains règlements ou même le ciblage, sont autant de sujets qui doivent demeurer dans un cadre national. Il est nécessaire de comprendre les spécificités nationales à des enjeux judiciaires, les règles de la guerre et le ciblage. Le fait de les mettre en œuvre de manière assez différente n'est ni surprenant ni important ; ce qui est fondamental c'est l'acceptation mutuelle et l'établissement de modes d'actions pragmatiques de coopération.

Les voies et moyens pour approfondir les relations 2017-2027

Si les relations franco-britanniques actuelles sont déjà approfondies et « automatiques » ⁽⁷⁾, tout doit être mis en œuvre pour poursuivre dans cette voie.

Trilatéralisation

C'était Harold Macmillan dans les années 1960 qui a le premier tenté de renforcer des relations de défense entre le Royaume-Uni, la France et les États-Unis. Dans un mémo vers ses collègues du cabinet, il a écrit en 1960 : « *Can what we want and what de Gaulle wants be brought into harmony? Is there a basis for a deal? Britain wants to join the European concern. France wants to join the Anglo-American concern. Can terms be arranged?... Are there offers we could afford to make? And could we persuade the Americans to agree* ». Presque 60 ans plus tard, il reste des arguments très forts en faveur d'une relation trilatérale approfondie (Londres-Paris-Washington). Mais trop souvent les discussions sont bilatérales – Washington-Londres, Washington-Paris, Paris-Londres –, et reflètent les environnements politiques de chaque pays. La défense offre une opportunité dans cette perspective à trois voix. Le P3 (USA, FR et UK) grâce au statut de membre permanent du Conseil de sécurité à l'ONU et à l'atout de puissances nucléaires, est un forum valable pour renforcer les relations, même s'il reste irrégulier et informel, et logiquement, focalisé sur les opérations. La *Trilateral Strategic*

(7) *Chief of Defence Staff UK* à Londres, le 6 février 2017.

Initiative, mis en œuvre par les trois armées de l'air, est un exemple de coopération trilatérale entre les armées qui fonctionne. Dans la mesure du possible, cette coopération devrait être élargie pour améliorer encore la compréhension mutuelle et l'efficacité. On peut même envisager, pour certains sujets, d'adopter une approche quadrilatérale. Par exemple, l'officier britannique en charge du soutien militaire à la sécurité de Londres, a initié une réunion quadrilatérale avec ses homologues à Washington, Paris et Berlin afin d'échanger et tirer les leçons communes aux quatre pays des événements passés. Le renseignement reste l'un des défis principaux de cette coopération. En effet, une option « *6 eyes* » n'est probablement pas très réaliste mais une approche plus cohérente du partage du renseignement entre la communauté de « *5 eyes* » et la France serait plus appropriée. Néanmoins, le partage du renseignement doit rester bilatéral et doit être une conversation bidirectionnelle. En effet, les États-Unis, le Royaume-Uni et la France ont tous des approches et tendances différentes dans le domaine du partage de leur propre renseignement. Des protocoles, des procédures et des passerelles techniques SIC existent mais pourraient être renforcés et mieux exploitées pour donner plus de résultats. Il faut également que la France partage son renseignement. Cette approche trilatérale ne doit pas gêner les relations bilatérales mais doit chercher à améliorer les capacités du P3 à opérer ensemble dans un contexte de sécurité et de défense qui l'exigera de plus en plus.

Coopération dans le domaine du « *Defence Engagement* »

Il est intéressant de noter qu'il y a beaucoup de points communs entre le modèle britannique de « *Defence Engagement* » (*DE*) et les missions françaises de coopération en Afrique francophone. Les réseaux des deux Nations sont bien établis et complémentaires, en Afrique en particulier, mais leur efficacité pourrait être mieux mise en valeur. Dans certains endroits, cette coopération n'est pas d'ailleurs nécessairement très nouvelle. Par exemple, au cours d'une mission de reconnaissance au Nigeria en 2006, l'auteur a assisté au déjeuner mensuel à Abuja au cours duquel les attachés de défense britannique, américain, français, allemand se rencontraient pour discuter des enjeux en cours et pour coordonner le soutien, que chaque Nation donnait aux forces militaires nigériennes. La décision récente du Royaume-Uni de créer un « *British Defence Staff* » au Nigeria pour soutenir l'Afrique de l'Ouest sera un point de contact important pour les forces françaises, que ce soient les forces prépositionnées ou les forces déployées en opérations.

Le réseau britannique (*DE*) s'élargit rapidement et l'axe entre Paris et Londres ne demande qu'à se renforcer. Le concept de ce rapprochement, en particulier sur les questions militaires et de sécurité, ne cessera de mûrir dans les domaines de la planification, de l'exécution et de l'exploitation.

Les armements et le niveau d'ambition

Approfondir la coopération dans le domaine des armements est une réponse évidente et pragmatique aux coûts croissants des équipements. Le Traité de Lancaster House a confirmé une telle approche. Il convient désormais de préciser les améliorations

de capacité et les économies, tout en protégeant les domaines relevant de la souveraineté nationale. Le modèle établi en septembre 2016, lorsque le Royaume-Uni et la France ont signé un accord pour mener conjointement le développement d'armes complexes (« *complex weapons* ») est un précédent important. L'accord prévoit que le projet et les exportations concernées ne seront pas un sujet aux négociations du *Brexit*. Pourtant, au-delà des armes complexes et du travail important sur la lutte contre les mines maritimes, l'ère *post*-Lancaster House n'est pas équivalente aux années 1960 ou 1970 quand le Royaume-Uni et la France ont coopéré pour développer l'avion Jaguar, l'hélicoptère Gazelle et le missile antichar Milan. Il est possible que le niveau de coopération nécessite d'être recalibré – ce qui ne sera pas facile étant donné les différences de systèmes d'acquisition et l'importance des exportations militaires pour les deux économies. Le *Future Combat Air System (FCAS)* reste un projet potentiellement important et son développement, au-delà du simple concept, refléterait une ambition réévaluée, quoique fragile par rapport aux échéances politiques à venir.

Anticipation et politique sécuritaire

Dans cette période qui a été profondément bouleversée dans de nombreux domaines, et dans l'intérêt de la prééminence des intérêts nationaux dans les processus complexes de prises de décision, il est crucial que le Royaume-Uni et la France recherchent conjointement des perspectives pour détecter les menaces et anticiper les domaines émergents. C'est en effet une évidence d'affirmer que dans la quasi-totalité des domaines, nous faisons face aux mêmes menaces. Il convient ensuite d'augmenter notre participation active et réciproque dans les processus comme nous avons commencé de le faire avec le programme « *CJEF*⁽⁸⁾ *Combined Horizon Scanning Approach* », qui concerne aussi bien les politiques de sécurité de la France et du Royaume-Uni que les recherches de coopération internationale. Le *SDSR 15* et le dernier *Livre blanc* français ont été un point de départ au moment de leur rédaction mais il faut maintenant approfondir le niveau de collaboration et développer des « *Joint Working Groups* », quel que soit le sujet. Au départ, il y aura quelques « *caveats* » (« restriction ») nationaux sur le partage des renseignements les plus sensibles. Une coopération, plus étroite entre « *Defence Intelligence Futures* » au Royaume-Uni et l'équivalent au sein de la Direction du renseignement militaire (DRM) en France, pourrait, à terme, donner d'excellents retours sur investissement. De la même manière, il pourrait être envisageable de faire participer le Royaume-Uni au groupe d'anticipation stratégique à Paris. Une telle coopération renforcerait la confiance mutuelle et permettrait de développer plus significativement une étude prospective pour anticiper les débats sur les intérêts nationaux et comprendre les points de divergence.

Une affinité conceptuelle

Le réseau des officiers de liaison et des officiers d'échange est efficace et parfaitement calibré. Alors que le *DE* est de plus en plus reconnu comme une carrière à part entière au sein du « *Ministry of Defence* », il est légitime de penser que de plus

(8) *CJEF* : *Combined Joint Expeditionary Force* ; Force franco-britannique mis en place en 2010.

Les possibles évolutions
de la relation franco-britannique d'ici dix ans

en plus d'officiers vont être attirés par une affectation à l'étranger et notamment vers la France. Des échanges, temporaires, entre les forces, quel que soit l'environnement, contribueraient à approfondir les relations personnelles et institutionnelles. Les relations entre pairs sont robustes et se renforcent jour après jour. Les Retex (Retour d'expérience) doivent devenir naturellement bilatéraux. Les officiers de liaison doivent pouvoir y assister tout comme leurs homologues de chaque pays.

Il serait également intéressant d'étudier une augmentation du nombre de participants de chaque pays aux cours majeurs – École de Guerre/*Advanced Command and Staff Course* et *HCSC/RCDS/CHEM*⁽⁹⁾. Il y aurait, peut-être, un intérêt d'examiner l'option d'accueillir les officiers généraux français à Robertson House⁽¹⁰⁾ pour la nouvelle formation des généraux britanniques – « *The Army Generalship Programm* ». Dans le même ordre d'idées, les Français peuvent proposer d'inviter les Britanniques pour participer à la formation des futurs officiers généraux à Paris. Un cours simplifié pour les officiers franco-britanniques à haut potentiel, à la mode du « *Capstone* » aux États-Unis, pourrait être valable aux niveaux personnels et institutionnels pour renforcer la connaissance mutuelle. Si on utilise les organisations qui existent déjà, les coûts devraient rester minimes.

Du reste, un *think-tank* franco-britannique au niveau politico-militaire pourrait être très utile s'il est établi d'une manière virtuelle pour réduire les coûts et, peut-être, construit sur le principe d'un *think-tank* actuel. Cette entreprise serait dédiée à l'examen des enjeux spécifiques qui pourraient affecter les relations franco-britanniques. Moins ambitieusement, le Royaume-Uni devrait examiner comment les écoles militaires présentent la France, aux plans politiques et militaires, à l'instar des officiers français du CHEM qui passent une semaine au Royaume-Uni afin de comprendre le contexte britannique.

La langue reste encore un défi pour les Britanniques et les leçons de français, qui ont été récemment ajoutées au *RCDS*, sont une bonne initiative, mais elles se déroulent trop tard dans la carrière d'un officier. La pression de temps à Sandhurst, à Cranwell et à Dartmouth⁽¹¹⁾ est immense mais c'est bien dans ces académies que l'apprentissage de la langue doit être commencé. Il faudrait cibler les étudiants en langue française des universités britanniques pour les encourager à s'engager dans les forces militaires et ainsi surmonter cette insuffisance. Un tel investissement dans la construction d'une affinité conceptuelle doit être poursuivi sous une forme « *bottom*

(9) *HCSC* : *Higher Command and Staff Course* ; formation dispensée à une trentaine d'officiers du grade de général de brigade ou colonel, dont 5 étrangers, et préparant les commandants de brigade à l'engagement sur les théâtres d'opérations extérieures. Basé à Schriivenham, au sein de l'Académie de Défense du Royaume-Uni, le *HCSC* est destiné à former les futurs chefs des forces armées.

RCDS : *Royal College of Defence Studies* ; centre de formation pour officiers supérieurs des forces armées britanniques et étrangères, civils de la défense traitant au niveau stratégique de sujets de sécurité internationale, afin de les préparer à exercer les plus hautes fonctions. Implanté au cœur de Londres, le *RCDS* est un organisme de rayonnement ouvert sur le monde. 50 des 100 auditeurs proviennent du *Commonwealth* et de pays alliés du Royaume-Uni.

CHEM : Centre des hautes études militaires.

(10) Robertson House accueille le *Centre for Army Leadership*.

(11) Sandhurst abrite la *Royal Military Academy* (le Saint-Cyr britannique) ; Cranwell, le *Royal Air Force College* (Salon-de-Provence) ; et Dartmouth, le *Birtannia Royal Naval College* (École navale).

Les possibles évolutions
de la relation franco-britannique d'ici dix ans

up » mais une impulsion « *top down* » pourrait être salutaire dans certains cas pour modeler les futurs cadres.

Construire un capital opérationnel

Les intérêts nationaux franco-britanniques ne convergeront pas tout le temps alors que les ressources dans le domaine de la défense seront toujours limitées. Dans ce contexte, il y a un intérêt mutuel à se soutenir l'un l'autre, d'une manière plus active, y compris par un déploiement limité sur le terrain, même si l'opération ne sert pas directement un intérêt national. Un tel déploiement contribuerait à renforcer une fidélité nationale et durable entre les deux pays. Il constituerait un capital opérationnel, dont il pourrait être fait usage de manière réciproque et qui aiderait à construire une capacité opérationnelle conjointe dans les années à venir (comme les opérations de l'Otan dans les pays Baltes). Un éventuel déploiement britannique pour soutenir un intérêt principalement français aiderait dès lors à affronter un scepticisme français, latent mais explicite, sur la volonté britannique de déployer les troupes au sol suite au rapport Chilcott ⁽¹²⁾.

Lancaster House II

Il semble qu'un second Traité de Lancaster House, ou un protocole d'accord additionnel, pourrait être approprié en 2020, à la suite des prochaines élections au Royaume-Uni, afin d'affirmer et peut-être d'amplifier les ambitions de cette coopération, et ainsi d'amender ce traité à la lumière des conséquences qui pourraient découler des négociations du *Brexit* et de la position du président des États-Unis. Il serait également opportun d'associer les nouveaux dirigeants des deux pays au traité lui-même. Il convient aussi de reconnaître la nécessité de protéger la liberté d'action de chacun pour opérer de manière indépendante afin de préserver des intérêts nationaux clairement identifiés. Pour le Royaume-Uni, l'exemple le plus évident est peut-être celui de la présence de sa force de dissuasion sur les îles Malouines. Pour la France, c'est sa présence actuelle en l'Afrique de l'Ouest.

Conclusion

L'imprévisibilité qui caractérise l'environnement actuel transforme en défi toute analyse prospective à dix ans. Néanmoins, il est clair que la relation franco-britannique, qui doit se nourrir d'une défense européenne intégrée dans l'Otan, doit prendre une importance croissante dans les dix années à venir au moment où prennent place le défi du *Brexit*, la présidence de Trump et l'idée d'une identité européenne de défense sans les Britanniques. Il y aura inévitablement des divergences, potentiellement des disputes, mais rien qui ne soit nouveau dans l'histoire commune des deux pays. Les relations franco-britanniques ont survécu à des moments qui étaient politiquement délicats auparavant, la guerre irakienne en 2003, par exemple. Et bien que les relations

(12) Rapport (John) Chilcot sur le bilan jugé désastreux de l'intervention du Royaume-Uni en Irak (www.iraqinquiry.org.uk/the-report/).

Les possibles évolutions
de la relation franco-britannique d'ici dix ans

aient pu être difficiles au moment des décisions mettant en cause les intérêts nationaux, les relations militaires, elles, n'ont jamais cessé.

Des deux côtés de la Manche, il y a une volonté explicite d'approfondir la relation qui est déjà forte et toutes les conditions institutionnelles sont réunies pour continuer de construire sur les fondations mises en place par le Traité de Lancaster House. Et dans un monde imprévisible, une relation de confiance procure un soutien mutuel et de plus, peut constituer une opportunité que d'autres pays pourront saisir au sein d'une coalition *ad hoc*, si le *CJEF* devait être déployé. L'expérience nous a montré que, dans le contexte européen, quand les intérêts français et britanniques sont en phase, il est alors possible de rassembler les autres partenaires sur le même objectif. Dans l'environnement actuel, cette proximité n'a jamais été aussi importante. L'axe franco-britannique pourrait également convaincre les États-Unis que l'Europe supporte plus efficacement le poids des responsabilités de défense et de sécurité. Inévitablement, il faudra prendre des risques, faire face aux idéologies politiques, aux rivalités profondément ancrées (économique et politique) et aux préjugés de circonstance. Mais il y a une appétence réelle pour élargir et pour approfondir les relations à travers les trois composantes et dans l'espace de sécurité. L'idéal serait de réussir à protéger ce partenariat si fort de deux Nations très complémentaires et d'empêcher que des complications imprévues autour des négociations du *Brexit* puissent avoir un impact désastreux sur leur coopération.

Éléments de bibliographie

CHALMERS Malcolm, « UK Foreign and Security Policy after Brexit », *RUSI Briefing Paper*, janvier 2017.

COOPER Duff, *Old Men Forget*, Rupert Hart Davis, 1953 ; 400 pages.

JOHNSTON Sandy, « France, the UK, the US and NATO », MOD paper, undated.

MEIJER Hugo, « Strategic Implications of Donald Trump's Election », *IRSEM Research Paper* n° 33.

PANNIER Alice, « The Anglo-French Partnership After the Brexit Vote: New Incentives and New Dilemmas », *Global Affairs*, 19 septembre 2016.

RAWNSLEY Andrew, « Mrs May discovers you can't be a bridge builder and a bridge burner », *The Guardian*, 5 février 2017 (www.theguardian.com/commentisfree/2017/feb/05/theresa-may-cu-donald-trump-role-britain-lonely).

Entretiens

- Bruno ALOMAR, journaliste.
- Alice PANNIER, Irsem (Institut de recherches stratégiques de l'École militaire).
- Lieutenant-colonel Antoine DE MEZAN DE MALARTIC, DGRIS (Direction générale des relations internationales et de la stratégie).

Vers une Union européenne de la sécurité et défense

Défis et perspectives de la politique allemande et de la relation Allemagne-France

Frank WACHTER

| Colonel (*Heer*), auditeur de la 66^e session du CHEM.

Défis actuels concernant la sécurité et la défense européenne

« (...) la défense européenne. C'est un sujet qui est vieux comme l'Europe, mais il se fait que, par l'Histoire, nous n'avons pas commencé par la défense, mais par l'économie et ensuite par la monnaie. Il est sans doute maintenant temps d'inverser le processus, non pas de remettre en cause ce que nous avons fait, mais de se dire que ce qui fait une solidarité c'est d'abord de nous préserver dans ce que nous avons d'essentiel et de pouvoir agir... Alors l'Europe doit se doter de toutes les capacités militaires, des ressources industrielles nécessaires, pour construire son autonomie stratégique... » ⁽¹⁾

Le caractère dramatique des mutations qui ont secoué les fondements de la politique de sécurité européenne fait apparaître que la Politique de sécurité et de défense commune (PSDC) demeure le maillon le plus faible du projet européen d'intégration ⁽²⁾. Des obstacles datant de longues années font obstacle à un rapprochement plus étroit, soit à cause de différences séparant les pays membres de l'Union européenne quant à l'appréciation qu'ils ont des menaces (Sud *vs* Est), soit en raison de leur culture stratégique respective voire, selon le cas, de leur culture politique respective (France *vs* Allemagne). On peut encore mentionner dans la liste des difficultés les divergences en matière d'objectifs et de priorités (cf. Irak 2003, Libye 2011) ou bien, dans certains cas, un manque de confiance et de solidarité. Le *Brexit* en est l'exemple le plus récent. L'ex-ministre allemand des Affaires étrangères (1988-2005), Joschka Fischer, a formulé avec des mots différents ce que déclarait le Président français, tel que cité précédemment : « L'Europe est vieille, riche et faible » ⁽³⁾.

Cette Europe est soumise aujourd'hui à une véritable épreuve de résistance dans le domaine de la politique de sécurité, notamment en ce qui concerne les mouvements de migration massive et la crise européenne des réfugiés pour laquelle aucune

(1) Discours du président Hollande à l'occasion de la Semaine des Ambassadeurs, publié le 30 août 2016, p. 10 (www.diplomatie.gouv.fr/IMG/pdf/30_08_f_hollande_discours_ambassadeurs_cle81c44c.pdf).

(2) Cf. à ce propos Arbeitskreis Internationale Sicherheitspolitik, *Ein Kompass für die GSV*, Friedrich-Ebert-Stiftung, Berlin, 2012, 8 pages.

(3) Cité d'après Erich VAD, « Starker Hang zum Appeasement » in *Cicero*, 26 mai 2016, p. 84.

solution durable n'a encore été trouvée. Vient s'ajouter à cela la crise de la dette européenne qui est loin d'être maîtrisée, de même que notre relation tendue avec la Russie encore en attente d'un règlement satisfaisant. Le conflit à l'Est de l'Ukraine s'éternise, tout comme la crise financière en Grèce. Ne considérant plus la sécurité de l'Europe comme un axe d'effort principal, les États-Unis se concentrent aujourd'hui sur la zone Asie-Pacifique et le Moyen-Orient. Dans le même temps, l'Europe est confrontée à la terreur islamique et au nouveau phénomène de migration terroriste étroitement lié. Le lien entre crise des réfugiés et terrorisme islamiste est d'autant plus prégnant que la majorité des migrants sont de jeunes musulmans.

Viennent s'ajouter à cette liste les incertitudes liées à l'élection de Donald Trump et au *Brexit*. Ce dernier événement n'aura toutefois pas d'impact direct sur la politique de sécurité, puisque la Grande-Bretagne a toujours été un pays membre engagé dans l'Otan. En revanche, les conséquences indirectes sont considérables. Dans les deux prochaines années, Londres et les autres capitales européennes dépenseront beaucoup de temps et d'énergie à gérer le processus de sortie de la Grande-Bretagne hors de l'UE – du temps qui aurait été plus utilement employé pour s'attaquer aux défis communs. En ce sens, le *Brexit* relève tout de même de la politique de sécurité européenne.

Ainsi, au cours des dernières années, de nombreux conflits et des phénomènes planétaires surgissent et surprennent par leur rapidité de leur évolution, réduisant l'importance de l'Union européenne comme acteur de la politique de sécurité. Pour les raisons que nous connaissons (dividendes de la paix, crise financière), les gouvernements ont perdu leurs capacités d'intervention militaire sur les théâtres d'opération et l'UE n'est pas à la hauteur des attentes placées en elle : elle n'est pas en mesure d'agir sur le terrain de la sécurité comme un acteur efficace dans le cadre de missions de grande envergure présentant un haut degré de complexité et s'inscrivant dans la durée. Elle était absente, même lorsqu'il aurait été nécessaire de démontrer rapidité et détermination face à certaines crises, ainsi en Libye ou au Mali.

Se rejoignant dans l'analyse selon laquelle la menace pesant sur la sécurité euroatlantique a aujourd'hui atteint un niveau inconnu depuis longtemps, l'Otan ⁽⁴⁾ et l'UE ⁽⁵⁾ ont engagé un changement de cap. L'Otan évoque un « univers de l'article 5 » de la dissuasion et de défense, l'UE un « *need to toughen up* » ⁽⁶⁾ et un moment opportun pour renforcer la Politique de sécurité et de défense commune (PSDC).

Nouvelle posture allemande

« Le consensus de Munich »

« Baisser davantage le seuil de responsabilités que nous sommes prêts à assumer, je dois vous le dire, ce ne sera plus longtemps possible ; mais en assumer davantage,

(4) Voir les décisions prises à Varsovie en 2016 ainsi que le nouvel accord Otan-UE.

(5) Federica MOGHERINI, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, publié à l'occasion du Sommet européen, Bruxelles, 28-29 juin 2016.

(6) Jean-Claude JUNCKER dans son discours sur l'État de l'Union tenu le 14 septembre 2016.

c'est ce à quoi nous allons d'abord devoir nous habituer »⁽⁷⁾. C'est en ces termes que le président de la République fédérale d'Allemagne, Joachim Gauck, en 2013, commente l'appel adressé à l'Allemagne à s'impliquer plus activement sur le terrain de la politique étrangère et de sécurité. Après avoir profité de nombreuses années de la sécurité que d'autres pays lui ont garantie, l'Allemagne, selon lui, devrait à présent assurer elle-même sa propre sécurité, de même que celle de ses alliés. Le temps où dominait la « culture de la retenue » est ainsi révolu, ajouta-t-il, plaidant pour une « culture de la responsabilité », qui devra être imposée, si nécessaire, par des moyens militaires.

Il s'empare de nouveau du sujet dans son discours d'ouverture de la Conférence de Munich sur la sécurité en 2014. Le message central qu'il y délivre, à savoir que l'Allemagne doit « s'impliquer plus tôt, plus résolument et de façon plus substantielle »⁽⁸⁾, a, en général, suscité une vive attention et a été bien accueilli. De façon plus critique, cet appel est assimilé à une invitation à s'engager militairement de manière plus prononcée.

Les discours du ministre fédéral des Affaires étrangères, Frank Walter Steinmeier⁽⁹⁾, et de sa collègue de la Défense, Ursula von der Leyen, prononcés respectivement en 2014 (« ... L'expectative... l'indifférence n'est pas une option pour un pays comme l'Allemagne... »)⁽¹⁰⁾ et en 2015 (« exercer le *leadership* au milieu de nos alliés »)⁽¹¹⁾ ont donné le coup d'envoi à un débat que beaucoup appelaient de leurs vœux depuis longtemps sur le rôle que doit jouer l'Allemagne à l'international.

Pour les partisans de la « culture de la responsabilité », il en va essentiellement de la fiabilité de l'Allemagne vis-à-vis de ses partenaires et alliés, sans pour autant susciter à l'étranger des attentes auxquelles l'Allemagne ne pourrait que difficilement répondre : « Assumer davantage de responsabilité oui, mais pas n'importe comment : dans l'anticipation et l'opiniâtreté ; proactif, mais sans surestimation de nos possibilités et toujours dans un cadre européen et international (...). »⁽¹²⁾

« Livre blanc 2016 sur la politique de sécurité et l'avenir de la Bundeswehr »

Paru exactement dix ans après le dernier *Livre blanc*, le *Livre blanc 2016*⁽¹³⁾ ne peut être compris en faisant abstraction de la conception modifiée que l'Allemagne se

(7) Discours du président de la République fédérale d'Allemagne Joachim GAUCK prononcé le 3 octobre 2013 à Stuttgart lors de la cérémonie donnée pour fêter l'Unification de l'Allemagne, p. 6 (www.bundespraesident.de/).

(8) Rede von Bundespräsident Joachim GAUCK anlässlich der Eröffnung der Münchner Sicherheitskonferenz am 31 Januar 2014 in München : « Deutschlands Rolle in der Welt: Anmerkungen zu Verantwortung, Normen und Bündnissen », p. 8 (www.bundespraesident.de/).

(9) Cf. COMMISSION EUROPÉENNE, *Plan d'action pour la défense*, 30 novembre 2016.

(10) Cf. Rede der Bundesministerin der Verteidigung, Dr. Ursula VON DER LEYEN, anlässlich der 50. Münchner Sicherheitskonferenz, München, 31 janvier 2014, p. 5.

(11) Cf. Manuskript der Rede der Verteidigungsministerin anlässlich der 51. Münchner Sicherheitskonferenz, München, 6 février 2015, p. 2 sq (www.bmvg.de/portal/a/bmvg!/ut/p/c4/PU1BCslwEHyLH8g29aLerAXxIiKC1kt).

(12) Rede von Außenminister Steinmeier bei der Münchner Sicherheitskonferenz 2015, p. 1 (www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2015/150208_BM).

(13) BUNDESMINISTERIUM DER VERTEIDIGUNG (Hg.), *Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr*, Berlin 2016.

fait du rôle qu'elle entend jouer et de son identité propre, aussi évoqué comme « consensus de Munich » et le principe d'« exercice du *leadership* au milieu de nos alliés ». Pour ce qui concerne la politique de sécurité allemande, le *Livre blanc 2016* fait découler de ces éléments la revendication de l'Allemagne d'agir et la volonté d'exercer une action modelante au niveau stratégique dans un environnement devenu encore plus complexe, plus volatile et plus dynamique. Comme tous les *Livres blancs*, celui-ci se veut également une approche prudente de la réalité. L'histoire des conflits de ces vingt dernières années avec des théâtres d'opération des Balkans à l'Hindou Kouch (Afghanistan) pour revenir vers l'Europe de l'Est appelle à suggérer deux tendances.

– Premièrement : Le monde poursuit sa mutation profonde, dont la violence récurrente a un impact sur la sécurité de l'Allemagne et celle de ses partenaires.

– Deuxièmement : L'environnement stratégique est devenu plus imprévisible et les conséquences éventuelles de nos actes sont encore plus imprédictibles que par le passé ⁽¹⁴⁾.

Personne ne pouvait prévoir la violence dont la Libye et la Syrie seraient la proie. Enfin, on sera amené à constater que la physionomie des conflits actuels aura, elle aussi, encore changé.

En dépit d'une inclinaison à l'apaisement et au pacifisme fortement marquée en Allemagne dans le domaine des Affaires étrangères et de la sécurité ⁽¹⁵⁾ le débat concernant le rôle de l'Allemagne et la politique de sécurité autour du processus d'élaboration du *Weißbuch* fait émerger une conscience du danger sur des bases rationnelles. À titre d'exemple, un appel du ministère fédéral de l'Intérieur est lancé en août 2016 pour constituer des stocks de survie pour 10 jours. Le pacifisme et le *post*-héroïsme constituent précisément, pour certains régimes autocratiques et certains opposants, une invitation à nous imposer des conflits et leurs formes.

Le nouveau *Weißbuch* n'est ni un commencement ni une fin ; il est un jalon sur la voie d'une réflexion stratégique reflétant la responsabilité internationale croissante de l'Allemagne et les obligations qui en découlent. L'avenir dira s'il est utile de développer plus avant dans cet esprit l'arsenal des mesures nécessaires à la réalisation de cet objectif¹⁶. Sur le plan intérieur, il importe plus que jamais de contribuer durablement à renforcer la résilience de notre société. Il s'agit en définitive de développer une « culture de la capacité à faire la guerre » ⁽¹⁷⁾, ainsi que l'a formulé le Chef d'état-major de l'Armée de terre [française] pour son pays : « Combattre là-bas pour nos valeurs, vaincre ici par nos valeurs. » ⁽¹⁸⁾. Mais pas seulement là. L'évolution des choses telle que montrée plus haut interdit à l'Europe de continuer à miser sur une vie dans

(14) Cf. Hilmar LINNENKAMP et Christian MÖLLING, « Das Weißbuch zur Verteidigungspolitik » in *SWP-Aktuell* n° 21, février 2015, p. 3.

(15) Cf. Erich VAD, « Starker Hang zum Appeasement » in *Cicero* du 26 mai 2016, p. 40 ; au sujet de la « *Postheroischen Gesellschaft* » [société *post*-héroïque] aktuell: Herfried Münkler, *Kriegssplitter*, Berlin 2015.

(16) Par exemple l'aptitude au *leadership* comme Nation-cadre et la mise à disposition de capacités critiques pour permettre la participation de partenaires internationaux.

(17) Josef JOFFE, « Neue Rolle der Bundeswehr? Ein bisschen Krieg » in *Zeit online* du 30 janvier 2014, extrait de l'hebdomadaire *Die Zeit*, édition juin 2014 (www.zeit.de/72014/06/bundeswehr-neue-rolle).

(18) Général d'armée Jean-Pierre BOSSER (Chef d'état-major de l'Armée de terre), *Le Figaro* du 21 mars 2016.

la paix et la sécurité sans, simultanément, accepter de répondre à l'impératif de défendre ses intérêts et ses valeurs – y compris dans l'espace européen ⁽¹⁹⁾.

Perspectives pour une coopération européenne de la défense pilotée par la France et l'Allemagne

Dans le contexte d'un environnement sécuritaire dégradé et avec une Allemagne prête à jouer un rôle plus actif sur la scène internationale, il est grand temps de renforcer notre solidarité et les capacités européennes afin de protéger plus efficacement nos frontières et les citoyens de l'UE et de contribuer à la paix et la stabilité dans notre voisinage. Pour cela, il semble indispensable d'orienter les réflexions et actions futures autour de trois axes principaux.

Transformer le Brexit en une nouvelle « fenêtre d'opportunité »

Il est encore difficile d'émettre des prédictions précises sur la façon dont évoluera la situation après le *Brexit*. Beaucoup d'experts ont annoncé que le *Brexit* n'aura pas d'impact considérable sur la politique de défense de l'Union européenne. Toutefois, l'UE perdrait l'une de ses grandes puissances militaires. À moyen et long terme, l'impact du référendum britannique sur la politique de défense de l'UE va largement dépendre des implications économiques du *Brexit* chez les autres États-membres et de l'attitude de ceux-ci vis-à-vis de la défense européenne ⁽²⁰⁾. Deux scénarios sont envisageables ⁽²¹⁾ :

- Le premier entérinerait l'échec de la Défense européenne. D'un point de vue économique, un ralentissement de la croissance dans les pays européens pourrait pousser ceux-ci à réduire leurs budgets de Défense et revoir leurs ambitions à la baisse. À l'échelle européenne, cela pourrait accroître les réticences de beaucoup de Nations à participer à des missions de la PSDC (le mécanisme *Athena* étant très limité, ce sont les États participants qui supportent l'essentiel des coûts des missions militaires). Au-delà du risque de contagion engendré par le *Brexit*, la sortie du Royaume-Uni pourrait également accroître les divisions et les tensions entre les États-membres restants, ce qui serait néfaste pour l'approfondissement de la défense européenne ou tout du moins pour le développement de nouveaux projets communautaires. Enfin, le Royaume-Uni cherchera probablement à renforcer l'Otan et à se concentrer sur ses partenariats bilatéraux pour remédier à sa perte d'influence sur le continent européen. Un grand nombre d'États considérant déjà l'Otan comme étant le garant de la sécurité européenne, le *Brexit* pourrait donc encourager nombre d'États à se concentrer encore plus sur l'Otan au détriment de l'Union. Un approfondissement de la coopération avec

(19) Cf. attentat du 19 décembre 2016 à Berlin et « En Europe, nous n'avons pas assez conscience du risque de guerre », Dominique DE VILLEPIN, cité à l'occasion de la publication de ses *Mémoires de paix pour temps de guerre*, 3 novembre 2016 (www.franceinter.fr/emissions/l-invite-de8h20).

(20) Le Royaume-Uni étant un contributeur net du budget européen à hauteur de 17 %.

(21) Cf. à ce sujet notamment Food for thought paper MBDA, *Le Brexit : implications pour le Royaume-Uni et l'Union européenne* (non publié 2016), p. 26 sq, de même que concernant le *Brexit* : *The Economist* du 24 septembre 2016, p. 49 sq de même que concernant le *Brexit* : « The fog of politics » in *The Economist* du 24 septembre 2016, p. 49 sq.

cette institution rendrait inutile l'existence de la PSDC et, à terme, pourrait avoir de graves conséquences sur l'autonomie stratégique des pays européens.

- Selon le second scénario, le *Brexit* aurait l'effet d'un électrochoc qui permettrait de relancer le projet de défense européenne. Malgré la sortie du Royaume-Uni, et les potentielles difficultés économiques que cela sous-entend, les budgets de défense nationaux augmenteraient afin de faire face aux menaces à la périphérie de l'UE. En outre, l'issue du référendum du 23 juin aura marqué le retrait d'un des pays les plus réticents à l'approfondissement de l'intégration européenne en matière de défense.

Plusieurs éléments nous amènent à penser que le second scénario est le plus probable et qu'il importe d'exploiter une « fenêtre d'opportunité » stratégique. Après le triple choc qu'ont représenté le *Brexit*, la tentative de coup d'État en Turquie et l'élection de Donald Trump, l'UE semble revenir à la conscience de ses valeurs et à sa volonté de les défendre offensivement ⁽²²⁾. Le *Brexit* serait donc l'occasion de relancer le projet de défense européenne en le basant sur la Stratégie globale récemment présentée par Federica Mogherini, Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité. Cela permettrait de rendre plus efficace et crédible la politique de défense européenne mais aussi de préserver l'autonomie stratégique du continent ⁽²³⁾.

**Revitaliser la « Politique de sécurité et de défense commune » (PSDC)
– vers une « Union européenne de la sécurité et défense » (UESD)**

« Il ne s'agit pas de créer une armée européenne. Il s'agit de mieux lier entre elles nos capacités européennes. » ⁽²⁴⁾

Au vu des restrictions dont font l'objet les budgets de la Défense et des mêmes menaces en Europe, il ne saurait y avoir d'alternatives à la coordination et l'harmonisation des capacités militaires. L'éventail de ces capacités mises en place et entretenues par l'Allemagne comme par les autres alliés européens – sauf surprise stratégique – continuera à subir la pénurie budgétaire. Car en dépit de l'augmentation de la plupart des budgets de la Défense, les marges de manœuvres financières des membres de l'Union européenne resteront dans l'ensemble étroites dans les domaines de la sécurité et de la défense, la situation économique de l'Europe continuant à imposer des limites claires aux dépenses publiques. Il faudra, du reste, compenser la sortie des Britanniques de l'Europe.

Néanmoins, en matière de défense, les dépenses cumulées des pays membres de l'Union européenne les placent au deuxième rang mondial. Mais, simultanément, avec plus de la moitié des dépenses militaires des États-Unis, elle n'atteint qu'un dixième

(22) Par exemple la suspension des négociations engagées avec la Turquie sur son adhésion à l'UE, la proposition de collaboration faite à Donald Trump sous réserve du respect des valeurs fondamentales ou l'intransigeance de l'UE vis-à-vis des conceptions britanniques du *Brexit* ; cf. à ce propos *Spiegel Online* du 26 novembre 2016, « Das neue Selbstbewusstsein der EU » (www.spiegel.de/politik/ausland/eu-nimmt-den-kampf-gegen-populismus-an).

(23) Cf. Federica MOGHERINI, *op. cit.*

(24) La ministre fédérale de la Défense, Dr. Ursula VON DER LEYEN, citée selon la revue de presse élaborée par la rédaction de la *Bundeswehr* en date du 28 septembre 2016.

du niveau capacitaire étatsunien ⁽²⁵⁾. Les dernières années ont mis en évidence que les pays européens n'ont pas la capacité militaire de durer, ni d'agir et qu'il existe de sérieuses lacunes capacitaires. On mentionnera à titre d'exemple les difficultés auxquelles s'est heurté l'Allemagne lors du déploiement longue durée des missiles sol-air à la frontière Sud de la Turquie ou bien les expériences faites par la France lors de l'intervention au Mali en 2013 dans les secteurs du transport aérien, du ravitaillement en vol et de la reconnaissance. Il en va de même pour l'engagement en Libye. Les raisons en sont évidentes. Au sein de l'Union européenne, les programmes de défense continuent d'être en concurrence, avec pour conséquences des redondances coûteuses dans le domaine des capacités militaires. Ainsi, il existe 20 programmes de véhicule blindé, six programmes différents de sous-marin, cinq programmes de missile sol-air ou cinq programmes d'avion de combat. En 2013, 84 % des achats de matériels et équipements ont été effectués dans un cadre national et un rapport du service scientifique du Parlement européen évalue à environ 26 milliards d'euros par an les coûts supplémentaires résultant d'un déficit de coopération dans le secteur de la défense européenne ⁽²⁶⁾.

Ces éléments devraient inciter à relancer un débat approfondi sur la création d'une « Union européenne de Sécurité et de Défense » (UESD) ⁽²⁷⁾. Sous l'égide de l'UESD pourraient être formulés des objectifs visant à l'intégration (future) de la défense européenne et à une coopération en Europe plus efficace et de meilleure qualité sur le plan de la politique de sécurité et de défense. Ainsi, elle constituerait le cadre actuel conceptuel au sein duquel pourrait être exigée tant la revitalisation de la « Politique de sécurité et de défense commune » (PSDC) que la reprise des efforts de défense des pays européens, toutes deux justifiées par la situation actuelle de la PSDC et par la réputation de l'Union européenne comme acteur en capacité d'agir dans le domaine de la sécurité. Il s'agit, dans le fond, d'une UE qui se conçoit également comme alliance de défense. S'inspirant de l'Union économique et monétaire, l'intégration de l'UE sur le terrain de la défense constituerait l'objectif final de l'UESD. L'état final recherché serait une **Europe de puissance** inspirée par le couple franco-allemand et construite par les pays qui le veulent et qui le peuvent.

Nous n'y parviendrons à moyen et long termes qu'en intensifiant progressivement la coopération et l'intégration dans le domaine de la défense, en homogénéisant les processus stratégiques, en rendant plus efficace les institutions, en élevant le degré d'interopérabilité et d'intégration des forces armées, en instituant un budget commun ⁽²⁸⁾ de même qu'en instaurant un marché commun de la défense qui soit concurrentiel. Doivent également figurer sur cette liste la planification et le développement communs et harmonisés de capacités ⁽²⁹⁾.

(25) Cf. *Planungsamt der Bundeswehr* [office de planification de la *Bundeswehr*], *Kurzstudie Europäisches Semester Verteidigung* (non publié), Berlin 2016, p. 16.

(26) Cité d'après le *Planungsamt der Bundeswehr*, *op. cit.*

(27) Cf. par exemple la Fondation Friedrich-Ebert, *op. cit.* *Le Livre blanc* [fédéral relatif à la politique de sécurité et à l'avenir de la *Bundeswehr*] désigne également comme « objectif à long terme » de la politique allemande une « union européenne commune de sécurité et de défense », voir p. 73.

(28) Cf. à ce propos les propositions faites actuellement par le ministre fédéral des Finances Wolfgang SCHÄUBLE (www.wallstreet-online.de du 19 octobre 2016) ainsi que Thierry BRETON, *op. cit.*

(29) Cf. COMMISSION EUROPÉENNE, *Plan d'action pour la défense*, 30 novembre 2016.

Il faudrait viser à instaurer un processus engageant mutuellement les pays membres ; lequel processus, conçu comme cycle, garantissant la transparence des planifications nationales des forces armées et dans le cadre duquel seraient débattus, coordonnés et harmonisés les budgets de défense et les plans d'acquisition de matériels et équipements militaires. Ainsi pourraient être apportées des réponses aux questions concernant les lacunes capacitaires et la planification financière, avec pour bénéfice une plus grande cohérence de la planification et du développement capacitaire dans le secteur de la Défense. Un facteur supplémentaire de cohérence résiderait dans le relèvement du degré d'engagement lié au dit processus en instituant l'obligation de se rendre compte mutuellement et en établissant des critères applicables aux achats et à la planification de matériels et équipements militaires ⁽³⁰⁾. L'adéquation de ce processus avec celui de planification de l'Otan devra être totale.

L'ensemble de ces mesures pourrait démarrer avec l'élaboration d'un « *Livre blanc* européen », devenant une publication stratégique prioritaire. Ainsi serait donnée l'occasion d'impulser à l'UESD une dynamique durable. Le but d'un tel document résiderait dans la définition de priorités concernant le développement de capacités militaires et dans l'identification de faiblesses, de lacunes et de remèdes à y apporter. La détermination d'un niveau d'ambition concret pourrait notamment constituer un vecteur de davantage de coopération dans le domaine de la planification capacitaire. De plus, le *Livre blanc* européen, expression de la nouvelle stratégie de l'UESD, déboucherait sur l'expression de besoins militaires actuels et actualiserait les *Headline Goals* existants.

Cette heure semble avoir sonné. Si le concept de Federica Mogherini (« Stratégie globale ») montre la voie, il n'est viable que si les pays membres de l'UE s'engagent de façon effective à lui donner vie. Dans le passé, la résistance des Britanniques à une politique de défense européenne commune était pour beaucoup un prétexte bienvenu pour brider les forces armées dans leurs capacités. Cela doit – et peut – changer.

Faire émerger une vision stratégique franco-allemande

Développer la PSDC dans cet esprit et se rapprocher de l'objectif d'une UESD supposent, dans une sage anticipation, d'exploiter toutes les possibilités offertes par le Traité de Lisbonne – le mot-clé étant la « Coopération structurée permanente (CSP) » ⁽³¹⁾. Dans ce cadre, tout dépendra de deux pays, qui devront continuer à évoluer pour atteindre ce but. Après le *Brexit*, l'Allemagne et la France seront les pays de l'UE disposant des deux plus puissantes armées. Ce seul fait leur confère un rôle décisif dans la refonte de la politique européenne de défense. Les autres pays membres observeront avec attention le comportement de l'Allemagne et de la France et s'engageront en fonction de l'impulsion donnée.

(30) Cf. à ce propos le *Planungsamt der Bundeswehr*, *op. cit.*

(31) Cf. BUNDESMINISTERIUM DER VERTEIDIGUNG (Hg.), *Weißbuch*, *op. cit.*, p. 33.

Pour l'Allemagne, mais aussi l'Italie et l'Espagne, la PSDC était considérée comme une étape parmi d'autres dans le processus d'intégration européenne. Le développement d'une défense commune se justifiait donc en tant que tel, à la lumière du projet plus vaste incarné par l'Union. La France, au contraire, a toujours perçu cette politique comme un projet avant tout opérationnel, visant à accroître la capacité d'intervention extérieure autonome des Européens, mais à travers une dimension intergouvernementale. En d'autres termes, Paris n'a jamais perçu cet outil comme un moyen devant renforcer l'intégration qualitative de l'UE dans une logique, à terme, supranationale (souveraineté nationale oblige).

Ainsi, face à la nécessité de réformer la PSDC, ces différentes approches se sont inévitablement déclinées en propositions allant dans des directions opposées. Par exemple, lorsque la France suggérait des initiatives visant à simplifier les procédures de lancement des opérations militaires de l'UE, notamment en réformant leur financement sur la base d'un budget commun, l'Allemagne demeurait sceptique, en y voyant une tentative de mettre les ressources de l'Union au service d'un agenda et d'un interventionnisme purement français ⁽³²⁾.

Divergentes, les positions françaises et allemandes ne sont pas pour autant inconciliables. En premier lieu, parce qu'elles ne reposent pas, comme dans le cas britannique, sur une hostilité de fond à l'idée que l'UE puisse développer, d'une manière ou d'une autre, une dimension militaire et devenir un acteur politique global. En second lieu, parce que la culture stratégique allemande est en train d'évoluer, en faisant de Berlin un acteur moins passif sur la scène politico-militaire mondiale.

C'est donc l'Allemagne qui pourrait converger vers la vision française de la PSDC, cette dernière étant incontestablement plus réaliste. Ce qui signifie que celle-ci est destinée à rester encore pour longtemps un projet de coopération interétatique, plutôt qu'un projet d'intégration. En d'autres termes : Armée européenne, non ; forces multinationales disposant d'une autonomie stratégique propre, oui. C'est dans cette logique coopérative que doivent être interprétées les nombreuses initiatives qui pourraient être relancées grâce au *Brexit*. Celle qui suscite le plus de curiosité est l'activation de la CSP suggérée très récemment par la France et l'Allemagne ⁽³³⁾. Elle doit s'adresser aux pays les plus vertueux et les plus volontaires sur le plan militaire en permettant d'aller de l'avant, la CSP ayant été pensée aussi pour contourner le veto des réticents. Le succès de cette politique dépendra avant tout de la capacité de la France et de l'Allemagne de continuer à converger et maintenir une vision stratégique commune et partagée.

Conclusion

« L'Europe se fera dans les crises et sera la somme des solutions apportées à ces crises. » ⁽³⁴⁾

(32) Cf. Thierry BRETON, *op. cit.*

(33) Voir le document stratégique franco-allemand, *Revitalisation de la PSDC. Vers une défense au sein de l'UE globale, réaliste et crédible* (non publié septembre 2016), p. 2.

(34) Jean MONNET cité d'après : *Mehr Europa in der Verteidigung, CEPS-FES Task Force Bericht, op. cit.*, p. 6.

Il reste donc à espérer que le moteur franco-allemand ne se remette pas à hoqueter, ni pendant l'année électorale de 2017, ni après. De toute façon, ce ne sont pas les idées de projets communs qui manquent pour les cinq à dix prochaines années ⁽³⁵⁾. Il faudra également attendre pour savoir si, au-delà de l'exemple franco-allemand, la coopération en matière de défense deviendra la norme et si la volonté politique en Europe sera à l'avenir suffisamment forte pour mettre ces principes en œuvre, par exemple lors du déploiement des « *EU Battle Groups* ».

Quoi qu'il en soit, le temps est venu d'un nouveau départ et nous devrions clairement formuler ce qui constitue le problème : la PSDC telle qu'elle a existé jusqu'à maintenant demeure le maillon faible de l'intégration européenne. Comme démontré supra, le Traité de Lisbonne exige beaucoup plus que cela et autorise une défense commune aux marges de manœuvre beaucoup plus importantes. Dans ce contexte, l'intérêt de l'UE à la poursuite d'une coopération étroite avec la Grande-Bretagne dans le domaine de la sécurité intérieure et extérieure (*special relationship*) s'en trouve augmenté. Faisant partie de l'Europe par la géographie, la Grande-Bretagne devrait donc naturellement y être associée, dans la mesure du possible (association possible à la PSDC/UESD comme pays tiers) ⁽³⁶⁾.

Des crises sont parfois nécessaires pour vraiment avancer. Nous sommes confrontés à une crise aux marches orientales de l'Europe en Russie et en Ukraine, à une crise dans le Sud-Est avec le totalitarisme djihadiste de l'« État islamique » en Syrie et en Irak, et à une crise chez nos voisins du Sud, le legs du « Printemps arabe », pas seulement en Libye. Pour finir, accentuée par le *Brexit* et les élections présidentielles aux États-Unis, la pression financière sous laquelle se trouve l'Europe n'est pas prête à baisser ⁽³⁷⁾. C'est la raison pour laquelle l'Union européenne se doit d'être beaucoup plus efficace dans le domaine de la défense. Cela signifie davantage de coopération, d'interopérabilité, de formation et d'équipements standardisés, davantage de commandement commun et une meilleure division du travail et répartition des charges, y compris un budget commun de la Défense ⁽³⁸⁾.

Dans ce domaine, les égoïsmes nationaux sont traditionnellement d'une grande férocité. Tout cela ne fonctionnera donc pas du jour au lendemain, nous aurons besoin de deux ou trois décennies, précisément le temps qu'il nous a fallu pour arriver à la monnaie commune, à l'euro. Et tous ne seront pas de la partie. Comme pour l'euro, nombreux seront ceux qui participeront, mais personne n'y sera obligé. Au contraire, le tout devra continuer à se développer avec pragmatisme par la base.

(35) Indépendamment des propositions figurant dans le document stratégique commun, l'Allemagne et la France veulent approfondir leur coopération dans quatre domaines capacitaires clé : ravitaillement en vol, communication satellitaire, cyberdéfense et drones.

(36) Environ 45 États non membres de l'UE participent à des opérations de la PSDC, 4 pays-tiers sont aussi participants dans les *Battle groups*. Cf. Thierry Tardy, *CSDP: Getting third states on board*, European Union Institute for Security Studies, mars 2014.

(37) Voir « Europäische Schuldenkrise », Ex. « France : Les tendances actuelles conduisent à une dette publique française supérieure à 100 % du PIB en 2020 » - Mot-clé « Respect des critères de Maastricht ».

(38) En additionnant les budgets européens, on dépasse de beaucoup la puissance financière de la Russie. Pacte de sécurité et Pacte de stabilité peuvent se renforcer mutuellement si les États-membres en ont la volonté politique et décident de mettre en place par exemple un Fonds européen de sécurité et de défense (FESD) comme ils ont su le faire pour le Mécanisme européen de stabilité (MES) à la suite des crises financières de 2008 et 2011. Cf. SCHÄUBLE et BRETON, *op. cit.*

En outre, nous avons, avant tout, besoin de plus d'accords multinationaux entre les différentes armées nationales portant sur des objectifs concrets – comme celui instituant l'état-major conjoint des marines belge et néerlandaise, le Commandement européen du transport aérien (*EATC*) implanté à Eindhoven, l'intégration de la brigade aéroportée néerlandaise à la Division de réaction rapide [allemande], l'accord entre les armées de terre allemande et polonaise, l'Escadrille de transport franco-allemande à Orléans. Les propositions contenues dans le document stratégique franco-allemand de septembre 2016 vont toutes dans cette direction ⁽³⁹⁾.

Il convient encore d'ajouter cette précision : des 27 pays membres de l'UE, 21 sont membres de l'Otan. Une défense européenne plus performante viendrait alors relever le degré de crédibilité de l'Alliance transatlantique. Les politiques de défense de l'Otan et de l'UE ne sont pas antinomiques ; elles ne devraient pas se considérer comme des concurrents mais au contraire se compléter, au vu des tâches communes que doivent assurer les États-Unis et l'Europe au sein de l'Otan. De plus, il existe des tâches non-Otan, les unes dédiées aux États-Unis, comme en Asie orientale, et les autres dévolues à l'Europe, comme en Afrique. La lettre commune des ministres de la Défense allemand, français, italien et espagnol d'octobre 2016 souligne cette approche : « *Given the current and foreseeable security environment, the EU will most probably have to launch missions of military and/or civilian character in regions NATO does not consider taking action, like the EU does and did e.g. Mali, Somalia, CAR, Congo, etc.* » ⁽⁴⁰⁾.

Quiconque, voulant préserver son autonomie de décision et d'action, préfère n'entretenir qu'une relation distante avec le partenariat transatlantique, devrait ne pas perdre de vue la situation géostratégique. Rapportée au globe terrestre dans son ensemble, l'Europe n'est qu'une petite parcelle de terre ; ce n'est donc qu'unie qu'elle a une chance d'être prise en considération. L'élection de Donald Trump à la Maison-Blanche renforce la nécessité pour l'Europe d'assumer davantage de responsabilité pour assurer sa propre sécurité. Quoi qu'il en soit, les États-Unis ne reverront pas à la baisse leurs exigences à l'endroit de l'Europe pour que celle-ci s'engage de façon plus prononcée au sein de l'Otan.

Si l'UE veut, à l'avenir, jouer un rôle de premier plan au niveau stratégique, elle ne doit pas seulement aller plus loin dans la mutualisation et la fédération de sa puissance militaire, mais également être en mesure de la déployer à court terme sur toutes les missions. De tels processus nécessitent du temps. L'Allemagne et la France devraient, avec un groupe de pays animés du même esprit, créer tant les capacités que les organes de décision nécessaires à de tels déploiements. C'est à cette seule condition que l'UE pourra, en dépit du *Brexit*, se réaffirmer au cours des années à venir comme centre de force dans le domaine de la sécurité en Occident. En conséquence, l'Europe est unifiée mais doit se présenter militairement comme un ensemble – l'UESD étant à cet effet la meilleure approche pour être à la hauteur des enjeux du futur.

(39) Cf. note 33.

(40) Voir à ce sujet la lettre commune des ministres de la Défense Jean-Yves LE DRIAN, Dr. Ursula VON DER LEYEN, Pedro MORENÉS et Roberta PINOTTI adressée en octobre 2016 à leurs homologues européens.

Vers une Union européenne de la sécurité et défense

Éléments de bibliographie

- BOSSER Jean-Pierre (Chef d'état-major de l'Armée de terre), « Combattre là-bas pour nos valeurs, vaincre ici par nos valeurs », *Le Figaro*, 21 mars 2016.
- BRETON Thierry, *Pour un Fonds européen de sécurité et de défense (FESD)*, juin 2016.
- BREUER Carsten et SCHWARZ Christoph, « Meilenstein, kein Endpunkt. Das Weissbuch als strategische Weichenstellung fuer deutsche Sicherheitspolitik », in *Internationale Politik* (2016), vol. 5, p. 83-87.
- Bundesaußenminister Dr. Frank-Walter STEINMEIER, Rede bei der Münchner Sicherheitskonferenz 2015 (www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2015/150208_BM).
- Bundesministerin der Verteidigung Dr. Ursula VON DER LEYEN, Rede anlässlich der 51. Münchner Sicherheitskonferenz, München am 06 février 2015 (www.bmvg.de/portal/a/bmvg/!ut/p/c4/PU1BCsIwEHyLH8g29aLerAXliKC1kt).
- Dies., Rede anlässlich der 50. Münchner Sicherheitskonferenz, München am 31 janvier 2014.
- Bundesministerium der Verteidigung (Hg.), *Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr*, Berlin, 2016.
- Bundespraesident Joachim GAUCK, Rede anlässlich der Eröffnung der Münchner Sicherheitskonferenz am 31. Januar 2014 in München: « Deutschlands Rolle in der Welt: Anmerkungen zu Verantwortung, Normen und Bündnissen » (www.bundespraesident.de/).
- Ders., Rede beim Festakt zum Tag der Deutschen Einheit am 3. Oktober 2013 in Stuttgart (www.bundespraesident.de/).
- Deutsch-französisches Strategiepapier, « Revitalisation de la PSDC. Vers une défense au sein de l'UE globale, réaliste et crédible » (unveroeffentlicht September 2016).
- LE DRIAN Jean-Yves, *Qui est l'ennemi ?*, Éditions du Cerf, 2016, 80 pages.
- Friedrich-Ebert-Stiftung, *Mehr Europa in der Verteidigung*, Report der CEPS Task-Force, Februar 2015.
- Dies., Arbeitskreis Internationale Sicherheitspolitik, Ein Kompass für die GSVP, Berlin 2012.
- Groupe de recherche et d'information sur la paix et la sécurité (GRIP), *La défense européenne après le Brexit : Mieux vaut tard que jamais*, 27 septembre 2016.
- Institut français des relations internationales (Ifri), « Le projet européen a-t-il un avenir ? » *Ramses 2017, Un monde de ruptures*, 2016, p. 140-163.
- JOFFE Josef, « Neue Rolle der Bundeswehr? Ein bisschen Krieg », in *Zeit online*, 30 janvier 2014, aus: *Die Zeit*, Ausgabe juin 2014 (www.zeit.de/72014/06/bundeswehr-neue-rolle).
- LINNENKAMP Hilmar et MÖLLING Christian, « Das Weißbuch zur Verteidigungspolitik », *SWP-Aktuell* n° 21, février 2015.
- LIPPERT Barbara et ONDARZA (VON) Nicolai, « Eine europäische „Special Relationship“. Leitlinien, Interessen und Spielraume der EU-27 in den Brexit-Verhandlungen », *SWP-Aktuell* n° 74, novembre 2016.
- MBDA, « Le Brexit : implications pour le Royaume-Uni et l'Union européenne » (unveroeffentlicht 2016).
- MOGHERINI Federica, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, hg. zum EU-Gipfel am 28-29 juin 2016.
- Planungsamt der Bundeswehr, *Kurzstudie Europaeisches Semester Verteidigung* (unveroeffentlicht, Berlin 2016).
- SCHULZE Hagen, *Die Wiederkehr Europas*, Siedler Verlag, 1990, 96 pages.
- SONNE Werner, « Deutschland macht mobil » in *Cicero*, 27 mai 2016.
- STAACK Michael, KRAUSE Dan (Hg.), *Europa als sicherheitspolitischer Akteur*, Opladen 2014.
- VÉDRINE Hubert, *Sauver l'Europe*, 2016, Liana Levi, 96 pages.
- VILLEPIN (DE) Dominique, *Mémoire de paix pour temps de guerre*, Grasset, 2016, 672 pages.
- VAD Erich, « Starker Hang zum Appeasement » in *Cicero*, 26 mai 2016.



■ **Penser les opérations**

RDN

Renforcement de la fonction « protection » à l'horizon 2030

Philippe DEDOBBELEER

| Colonel (air), auditeur de la 66^e session du CHEM.

Profitant des dividendes de la paix, la protection n'a pas toujours été au cœur des préoccupations de la défense et de la sécurité sur le territoire national ⁽¹⁾. Or, les actions du pseudo-État islamique, concrétisées dans notre pays par les tragiques événements de l'année 2015, tout comme la résurgence des États-puissances, nous ont rappelé que la sûreté et la sécurité ne sont jamais définitivement acquises, bien au contraire.

De l'analyse des menaces qui perturbent la sécurité de la Nation, associée à celle des principes à respecter pour garantir la meilleure protection, un état des lieux de cette fonction stratégique sera fait. De là sera établie une série de propositions, portant sur les capacités transverses ⁽²⁾, essentiellement d'ordre technique et du ministère des Armées, qui vise à renforcer dans les dix prochaines années la protection sur le territoire national.

Une menace ⁽³⁾ durable et globale

La menace sur le territoire national est permanente et évolutive. Elle est globale car nos centres d'intérêt sont multiples, variés et de plus en plus interdépendants.

Une menace durable : l'islamisme radical et les États-puissances

Les menaces se rapprochent de l'Europe et de ses frontières. Le contexte sécuritaire se caractérise par deux lignes de conflictualité, distinctes mais non disjointes, qui s'ajoutent l'une à l'autre : l'islamisme radical et le retour des États-puissances, traditionnels ou émergents.

En s'attaquant à nos valeurs et à nos repères, le djihadisme transnational cherche à miner notre cohésion et notre capacité de résilience nationales, ainsi qu'à délégitimer l'État-Nation. L'idéologie transcende les mouvements, dont les formats, les structures et les modes d'actions s'adaptent en fonction de l'espace et du temps, afin de poursuivre son expansion. Même si les armées occidentales réussissent à affaiblir

(1) Il comprend la métropole, les départements et les collectivités d'outre-mer, les espaces aériens associés, les approches maritimes ainsi que les Zones économiques exclusives (ZEE).

(2) En raison de l'exhaustivité des capacités mises en jeu, nous avons choisi d'insister sur les capacités techniques communes ou à partager qui concourent *de facto* à une approche globale de la fonction « protection ».

(3) La menace est le produit de deux facteurs : celui de l'impact d'une agression qui se combine avec celui de sa probabilité.

Al-Qaïda et *Daech* sur leur terrain, la menace risque de pivoter géographiquement. Les mouvements djihadistes sont en mesure, à partir de leurs sanctuaires, d'orchestrer des attentats sur notre sol, dont l'ampleur ou le degré de sophistication peuvent être significatifs.

En parallèle de l'émergence ou de la réaffirmation de grandes puissances régionales ⁽⁴⁾, la Chine et la Russie affichent, avec des actions concrètes et des investissements ambitieux, une volonté politique affirmée et une contestation de l'ordre international établi. Plus préoccupante car plus proche, la Russie a réinvesti dans son appareil de défense et s'évertue régulièrement à mettre en avant ses capacités militaires étendues, en effectuant des manœuvres aériennes ou sous-marines à l'abord de nos frontières. Elle a par ailleurs déployé, y compris en Baltique, un réseau de systèmes de défense antiaérienne hors d'atteinte de nos moyens aéroportés. Cette situation aboutit à une inversion du rapport de forces à notre désavantage, d'autant plus perturbante que la crédibilité de l'Alliance atlantique tend à être remise en cause par certaines des déclarations du nouveau Président américain.

Une menace inéluctablement globale

De surcroît, indépendamment ou non des moyens financiers et humains dont elle dispose, l'agression profite des progrès technologiques, souvent facilement accessibles, dont les effets peuvent être inattendus et démultipliés par la connectivité offerte par l'omniprésence des Nouvelles technologies de l'information et de la communication (NTIC). Les derniers mois abondent d'exemples d'attaques cyber. D'origine étatique ou individuelle, elles peuvent être dévastatrices sur le plan technique, mais aussi économique, social ou politique.

L'Espace, extension du milieu aérien mais aussi cyber, n'est plus forcément le domaine réservé de grandes puissances. Des essais de satellites se déploient et leur miniaturisation s'accroît. Le trafic des engins spatiaux, qui deviennent aussi des armes, s'intensifie tandis que leur détection et leur identification se complexifient.

N'oublions pas la prolifération des objets nivelants, opportunités clé en main pour l'ennemi, tels que les mini-drones : bon marché, d'une facilité déconcertante d'utilisation, télécommandables ou programmables, ils sont capables de transporter des charges utiles qui peuvent échapper aux capacités défensives. Ne sous-estimons pas non plus les matières NRBC (Nucléaire, radiologique, bactériologique, chimique) qui peuvent aussi être utilisées par des apprentis sorciers qui récupèrent des informations sur *Internet*.

Au bilan, la France est susceptible d'être victime sur son territoire d'agressions de faible et de haute intensité, directe ou indirecte, allant de l'acte isolé à l'opération majeure ⁽⁵⁾, provenant d'un individu isolé ⁽⁶⁾ comme d'une puissance étrangère.

(4) L'Iran par exemple, avec une ambition nucléaire, avérée ou non.

(5) Sans oublier l'action commando des « arrivants » ou des « revenants », aguerris aux actions militarisées.

(6) Individu n'appartenant à aucun mouvement, qui agit, sans aucune conviction idéologique, par seul mimétisme.

L'interdépendance croissante des domaines, conséquence de leur connectivité exponentielle, concourt à une globalité de plus en plus marquée de la menace.

Des principes de protection inamovibles

Aptitude à faire face à tout type d'agressions, en tout temps et en toutes circonstances, selon une approche intégrée à l'échelle du pays, telle doit être la qualité première de la fonction stratégique « protection », garante de notre sécurité et de notre souveraineté, plus que jamais indissociable des autres fonctions stratégiques.

Le maintien d'une protection efficace

La Nation doit contrer des agressions, de faible comme de haute intensité, novatrices ou non, qui par leur mode d'actions, peuvent atteindre plusieurs cibles simultanément ⁽⁷⁾. Elle doit donc disposer en permanence de tout le spectre des capacités, soient les ressources humaines, les équipements, les soutiens, les organisations, les doctrines et les entraînements. La protection doit rester innovante afin d'avoir une longueur d'avance sur la menace : de lourds efforts doivent être consentis dans le domaine prospectif (études amont, recherches) et celui des opérations d'armement (accélération des calendriers).

Une organisation agile, stable et du bon niveau

Les compétences et les moyens dont dispose la Nation pour assurer sa protection doivent être performants, complémentaires et interopérables. Pour former un ensemble cohérent et efficace face aux menaces, une gouvernance appropriée est indispensable. Globalité et connectivité exponentielle de la menace exigent les mêmes caractéristiques en réponse. Celle-ci peut couvrir plusieurs dimensions, niveaux ou milieux aux frontières poreuses ⁽⁸⁾ et exige une interopérabilité structurelle, humaine, matérielle, horizontale et verticale. La multiplication des échanges est non seulement primordiale mais aussi inévitable ; elle doit être maîtrisée pour rester un facteur de puissance et ne pas devenir un facteur de vulnérabilité. La recherche de synergies et l'optimisation restent indispensables dans la durée, aussi bien dans l'anticipation que dans l'action, afin de s'adapter en permanence au contexte évolutif des menaces (en particulier des moyens utilisés). En raison de son caractère interministériel et interallié, elle suppose une mise en cohérence par le haut et/ou par le bas.

On le voit, la protection de la Nation doit s'appuyer sur une organisation multidimensionnelle s'appuyant davantage sur les autres fonctions stratégiques. La dissuasion reste en effet essentielle face au retour des États-puissances et à la prolifération nucléaire. De même, la fonction « connaissance et l'anticipation » doit désormais prendre en compte un nombre croissant de signaux faibles. Finalement, la Nation tout

(7) L'impact peut être à la fois économique, social, technique, politique, militaire et/ou sociétal.

(8) Paix, crise, guerre – Défense, sécurité – Intérieur, extérieur – Politique, diplomatique, économique, social, culturel, religieux – Interministériel – Milieux terrestre, maritime, aérien, spatial, cyber – Centralisé, décentralisé – Stratégique, opératif, tactique.

entière doit s'approprier le nouveau paradigme dans lequel nous vivons, conséquence de l'augmentation de la menace, tant par sa fréquence que par sa violence.

Forces et faiblesses de la fonction stratégique « protection »

En parallèle de la dissuasion nucléaire, la France a construit une sauvegarde générale. Autant elle a constamment fait évoluer ses Postures permanentes de sûreté aérienne (PPS-A) et de sauvegarde maritime (PPS-M), autant elle a baissé la garde depuis la fin de la guerre froide dans la protection sur le sol. La prise en compte trop récente de l'extension des menaces à de nouveaux milieux (cyber, spatial) a aggravé les faiblesses d'une posture réellement apte à faire face à tous les défis et enjeux.

Des sauvegardes aérienne et maritime et une organisation interarmées de défense rodées

La PPS-A est une mission confiée à l'Armée de l'air et placée directement sous l'autorité du Premier ministre, qui a pour objectif de garantir la souveraineté et la sécurité de l'espace aérien national. Agissant dans un contexte fortement interministériel, l'Armée de l'air met en œuvre 24 heures sur 24, en tant que primo-intervenante, un dispositif chargé d'évaluer la menace dans l'espace aérien national et de s'opposer ⁽⁹⁾ à toute agression opérant dans la troisième dimension. Initialement bâti pour interdire ou intervenir contre toute pénétration jugée hostile de l'espace aérien, massive ou non, ce dispositif de police du ciel constitue un ensemble complet et cohérent comprenant des structures de commandement, des centres de détection et de contrôle, des systèmes de surveillance, d'information et de communication ainsi que des plots d'alerte intervenant dans la troisième dimension.

Concomitamment, la Marine nationale assure la PPS-M qui répond au même besoin dans le milieu maritime selon des principes équivalents. Afin d'assurer la souveraineté et la sécurité de nos approches maritimes ainsi que la protection du littoral à partir de la mer, la PPS-M agit à l'interface du milieu terrestre et aéro-maritime, *via* un dispositif en strates successives du littoral à la haute mer, dont les mailles se resserrent à mesure que l'on se rapproche des côtes nationales. Son champ d'action va, à l'instar de la PPS-A, de la prévention à l'intervention.

En reliant les capteurs, les centres de détection et de contrôle, et le Centre national des opérations aériennes, le Système de commandement et de conduite des opérations aériennes donne en temps réel la situation aérienne générale. Après avoir renforcé les partenariats avec nos pays voisins à la suite des attentats du 11 septembre 2001, s'être adapté aux menaces « plus lentes ou plus discrètes » ⁽¹⁰⁾ de l'époque par l'ajout de plots « hélicoptère » aux plots « chasse », la PPS-A est aujourd'hui capable d'intercepter avec réactivité ⁽¹¹⁾ les aéronefs allant de l'ultraléger motorisé (« petit », « lent ») à l'avion de chasse (« moyen », « ultrarapide et vélocé ») en passant par l'avion

(9) Contrer, neutraliser voire détruire.

(10) Ultralégers motorisés, parapentes.

(11) Dans un délai inférieur à 15 minutes.

commercial (« gros », « rapide »). Parallèlement, la surveillance du littoral et de ses approches est en particulier assurée au travers de sémaphores répartis le long de nos façades maritimes, complétés par des capacités aéromaritimes qui agissent dans la profondeur au large de nos côtes. En complément de ces actions de prévention, la Marine nationale met en œuvre une panoplie de moyens couvrant l'ensemble du volet intervention (démontage, neutralisation de drones, arraisonnement de navires, contre-terrorisme).

À la différence des milieux aérien et maritime ⁽¹²⁾, les armées ne sont pas primo-intervenantes en milieu terrestre sur le territoire national, partagé en sept zones métropolitaines et cinq ultramarines qui relèvent de la compétence d'un Préfet de zone de défense et de sécurité. Leur intervention s'inscrit dans le cadre d'une demande de l'autorité civile. L'Organisation territoriale interarmées de défense facilite le dialogue civilo-militaire. Miroir de la chaîne décisionnelle préfectorale, cette structure permanente à trois niveaux ⁽¹³⁾ repose majoritairement sur les capacités des armées pour compléter, lorsque nécessaire, l'action des services publics. La rapidité du déploiement du dispositif *Sentinelle* (10 000 militaires en 48 heures), au lendemain des attentats de janvier 2015, témoigne de l'efficacité de cette organisation.

Des failles dans nos moyens de détection aérienne et maritime.

Des capacités de protection cyber, spatiale et terrestre encore beaucoup trop jeunes

Le rythme des modernisations et de renforcement des systèmes de surveillance contribuant aux postures permanentes de sûreté aérienne et de sauvegarde maritime n'a pas été aussi rapide que souhaité ces vingt dernières années, principalement dans les capacités de surveillance. Les insuffisances constatées dans les volets cyber, spatial sont naturellement le fruit de leur manque de maturité et pour le volet terrestre, d'une pratique limitée au Plan *Vigipirate* depuis 1995, et à l'effacement progressif du concept de défense opérationnelle du territoire.

La faiblesse première des PPS-A et PPS-M est due à l'insuffisance qualitative et quantitative de couverture de détection. Celle-ci est la conséquence de l'absence de radars dans certaines zones, de leur obsolescence ou du besoin régulier de renforcer la détection au regard de l'évolution très rapide de la menace. Dans le domaine aérien, certains planchers ou plafonds de détection sont ainsi en partie inadaptés aux domaines de vols des engins actuels, dont les plus rustiques peuvent décoller à partir d'une zone sommaire quelconque et se diriger potentiellement vers n'importe quelle cible.

Échappent également à la vigilance du système de détection des engins spatiaux *Graves* ⁽¹⁴⁾, dont est doté le pays depuis 2005, les petits objets qui prolifèrent depuis peu dans l'espace extra-atmosphérique. De plus, le système d'information (SI) de trajectographie satellitaire est alimenté par les pays qui acceptent de diffuser leurs données spatiales et d'enrichir le catalogue commun des objets en orbite. L'expérience

(12) Hors situations d'urgence où des vies humaines sont en danger.

(13) Chef d'état-major des armées au niveau central, officiers généraux de zones de défense et de sécurité (dont commandants supérieurs) au niveau zonal, délégués militaires départementaux au niveau départemental.

(14) *Grand réseau adapté à la veille spatiale.*

nous montre que la base de données est loin d'être exhaustive pour des raisons compréhensibles de souveraineté. Pourtant, certains événements mettent en évidence que nos systèmes spatiaux peuvent être approchés à des fins hostiles et que nous n'avons aucun moyen de défense dans ce domaine. Au bilan, même si la France bénéficie d'une certaine résilience dans ses capacités spatiales de télécommunications et d'observations ⁽¹⁵⁾, elle ne dispose que d'une capacité limitée dans le milieu extra-atmosphérique qui concourt pourtant directement à la fonction stratégique « protection ».

S'agissant du cyber, des progrès significatifs ont été réalisés ces cinq dernières années aussi bien sur le plan organisationnel, technique qu'en matière de ressources humaines. Mais la tâche à accomplir reste de taille tant les défis sont multiples. Le maintien à un haut niveau de sécurité exige un financement soutenu et un très haut niveau de compétences. La maîtrise systémique est par ailleurs rendue difficile par une ouverture inéluctable de flux pour des besoins d'échanges externes croissants. Enfin, les attaques se multiplient tant la proie est facile et à la portée du moindre *hacker*. La liste n'est pas close...

Au sol, les armées continuent de répondre avec brio au besoin de renforcement des forces de sécurité intérieure. Mais le changement d'échelle, imposé à la fois par la nature des événements et par la durée de la posture en réponse, a mis en lumière des divergences civilo-militaires (notamment dans les modes d'actions en planification comme en conduite, dans les choix relatifs aux moyens de communication) dont les plus urgentes ont été résorbées en 2015-2016.

La fin de la conscription, l'évolution vers des missions expéditionnaires des forces armées et la réduction constante des effectifs, ont amené les armées, directions et services, durant la période 1995-2015, à réduire le niveau de protection des sites militaires dont ils avaient la responsabilité. En conséquence, cela s'est traduit par une baisse du nombre de militaires dédiés à cette tâche et au remplacement d'unités militaires par des sociétés civiles de sécurité pour la protection de certaines installations. Enfin est constatée une insuffisance notable des moyens matériels de protection ⁽¹⁶⁾ en lieu et place du personnel, en particulier en matière de dispositifs de contrôle d'accès, de détection d'intrusion et de vidéosurveillance (CA-DI-VS). L'année 2015 a révélé une situation dramatique dans ce domaine.

Une PPS, globale et intégrée, à l'échelle de la Nation

La protection de la Nation, des citoyens dont il s'agit de la première attente, tout comme des installations vitales, méritent des efforts de tous les instants. Le principal défi à venir est de construire une posture réactive de sûreté, agile, intégrée et globalisée, à partir des postures déjà existantes ou en cours de construction. Cette « méta-posture » impose d'appréhender la protection dans une approche interarmées, interministérielle et souvent interalliée. Les déclinaisons capacitaires transverses à

(15) Chiffrement des communications, durcissement des fréquences utilisées au sol, etc.

(16) Infrastructure, barreaudage, blindage, dispositifs de contrôle d'accès, de détection d'intrusion et de vidéosurveillance.

caractère technique seront plus particulièrement décrites dans les recommandations générales qui suivent.

Moderniser et renforcer les postures de sûreté aérienne et maritime

Les PPS-A et PPS-M doivent désormais constamment être maintenues à un haut niveau de performance ⁽¹⁷⁾, afin non seulement de poursuivre les rôles pour lesquelles elles sont conçues, mais aussi de s'adapter aux nouveaux modes d'actions hostiles. D'une manière générale, il est crucial de stopper les dérives calendaires des opérations d'armement qui concourent à rénover ou à acquérir les équipements permettant de réaliser ces missions ⁽¹⁸⁾.

Les nouveaux radars de circulation et défense aériennes, qui concernent dorénavant les trois armées, méritent une attention particulière en raison de l'urgence de leur déploiement. Ils minimiseront le risque de perte de couverture de détection, diminueront le plancher et augmenteront le plafond de détection dans les zones couvertes en renforçant la capacité de veille lointaine dans l'espace aérien au-dessus des approches maritimes nationales. Devra être programmée dès maintenant leur rénovation afin de continuer à faire évoluer les capacités de détection face à des moyens de plus en plus furtifs ou hypervéloces. En parallèle, l'amélioration des capacités de la chaîne sémaphorique doit se poursuivre avec l'acquisition de moyens de détection supplémentaires, plus performants et/ou innovants, afin d'éviter toute lacune dans la surveillance de la façade maritime nationale.

La France doit rester dynamique dans sa participation au programme *ACCS* ⁽¹⁹⁾ de l'Otan. En partageant les procédures, dans le respect des politiques nationales de sûreté et d'engagement du feu, et en communalisant les outils mis en œuvre, ce projet majeur pérennise l'interopérabilité avec nos partenaires de l'Otan qui permet d'anticiper en amont la menace aérienne dans l'espace aérien européen, le tout selon une approche systémique de sécurité. En parallèle, il est tout aussi important de continuer à développer les capacités d'interception et de neutralisation de drones, aussi bien sous-marins qu'aériens, tout en veillant à les intégrer au mieux à ces systèmes de surveillance et d'alerte.

La guerre électronique est une priorité croissante eu égard à la prolifération tous azimuts technologique. Il est impératif de prévoir systématiquement des capacités « anti-déni » dans tous les domaines, car nous devons être en mesure de garantir la disponibilité de nos moyens en zone électroniquement hostile. Dans ce cadre, des moyens de lutte antimissile ⁽²⁰⁾ doivent équiper nos radars, tout comme nos systèmes doivent toujours être capables de récupérer les signaux émis par le système de géolocalisation

(17) Aussi bien dans le domaine de l'organisation, de la technique et des compétences.

(18) Y compris les plateformes (avions de combat, de surveillance aérienne ou maritime, patrouilleurs maritimes, etc.), leurs armements (missiles, canons, etc.) et équipements de commandement et de contrôle (radios, radars, liaisons de données tactiques, etc.).

(19) *Air Command and Control System*, en cours de mise en service opérationnelle.

(20) Brouillage, leurrage.

GPS ⁽²¹⁾, demain *Galileo*. Réutiliser plus massivement les références horaires issues des horloges atomiques est un autre exemple de résilience des systèmes face à la perte du système *GPS* ou *Galileo*.

Poursuivre la construction des postures cyber, spatiale et terrestre

La montée en puissance des capacités agissant dans les milieux cyber et spatial doit être poursuivie afin de lutter contre des menaces qui peuvent toucher tous les secteurs de la société. L'édification d'une posture de sûreté terrestre, à l'instar et en parallèle des postures aérienne et maritime, est aujourd'hui possible. L'approche globale a permis des progrès significatifs dans les volets cyber et spatial. Elle s'est traduite, sur le plan organisationnel, par la création de commandements spécialisés ⁽²²⁾ qui assurent une gouvernance d'ensemble et une cohérence des actions au sein du ministère. Ils ont défini des politiques générales de milieu qui constituent un édifice solide pour les postures à finaliser, qui impliqueront les armées, directions et services.

Dans le domaine du cyber, milieu virtuel complexe, il convient en priorité de continuer à accroître le niveau en ressources humaines, notamment sur le plan qualitatif, au profit des forces armées et des services. La consolidation du pôle de compétences (réunissant défense, universités et entreprises), récemment constitué, passera par la capacité du ministère, mais aussi de l'État, à recruter et à fidéliser des spécialistes de très haut niveau.

L'effort porté sur la prise en compte *ab initio* du maintien en condition de sécurité (MCS) de tout SI (y compris micro-logiciel) doit rester la règle dans la conduite des projets. Ceci concerne au premier plan le volet cyber mais aussi le volet spatial, partiellement « intégré » au premier. L'implication systématique en amont des acteurs *ad hoc* est tout aussi nécessaire pour consolider la définition du périmètre du MCS dans son futur environnement technique que pour concourir à l'intégrité du système dès sa mise en service.

Naturellement, l'approche systémique est source d'efficacité dans la prise en compte du besoin de protection. Elle implique de toujours maîtriser dans leur globalité les architectures de sécurité, des systèmes d'information et de communication, avec des ressources techniques judicieusement réparties sur le territoire (« *Cloud defense* » ⁽²³⁾). Celles-ci seront combinées à une capacité maximale d'intervention sécurisée à distance (télé-action) sur les équipements et les logiciels par les équipes en charge de leur mise en œuvre et de leur soutien. Toujours dans ce cadre, il est pertinent de canaliser les flux croissants, entrants comme sortants, de nos réseaux au travers de passerelles dont la gestion est assumée par des experts, ceci afin de garantir au mieux leur sécurité (disponibilité, intégrité, confidentialité).

(21) *Global Positioning System*.

(22) Respectivement en 2010 pour le spatial et en 2016 pour le cyber.

(23) *De facto* résilient puisque par nature redondé.

Renforcement de la fonction « protection » à l'horizon 2030

Une analyse générale, couvrant tous les volets (stratégique, industriel, économique, technologique, etc.), mérite d'être conduite, autant que de besoin, afin de s'assurer dans le temps, eu égard à l'évolution des agressions, de la pertinence de la politique générale retenue dans le développement des architectures nationales cyber de défense et de sécurité. Les moyens de chiffrement, socle historique du cyber (volet protection), ont depuis leur origine, pour les besoins gouvernementaux, été réalisés par le « complexe militaro-industriel » français ⁽²⁴⁾. Il faudra s'interroger sur le besoin d'étendre ou non cette politique générale ; en clair, de redéfinir ce qui doit appartenir à notre socle cyber-protection ⁽²⁵⁾. Quoi qu'il en soit, il convient impérativement de préserver la Base industrielle technologique de défense (BITD) qui concourt directement au socle actuel (industries des composants et des logiques cryptologiques). En outre, même si la question relative à la recherche de partenariat pourra être posée (en particulier pour des questions de partage des coûts), il faudra rester vigilant dès lors que l'on touche aux fondamentaux de la souveraineté nationale. Enfin, l'expérience montrant sans cesse qu'une des failles dans la protection cyber est d'origine humaine, le développement d'outils qui maximisent la sécurité, en toute transparence pour l'utilisateur, est à promouvoir.

Dans le domaine spatial, le renforcement des capacités de résistance au brouillage d'une part, une meilleure connaissance des objets stellaires pour identifier la menace, caractériser l'agresseur et protéger les moyens spatiaux d'intérêt stratégique d'autre part, sont les priorités. Ces dernières passent par le renforcement de la détection radar et de la situation spatiale en temps réel. Les études prospectives relatives aux moyens de neutraliser les satellites menaçants devront aboutir à des choix physico-financiers avant 2030.

S'agissant du domaine terrestre, le ministère de la Défense a entrepris dès 2015 une opération d'ensemble qui vise à redynamiser sa propre protection. Pour cela, il fait réaliser des travaux d'infrastructure afin de renforcer la résistance physique de ses bâtiments et/ou déployer parallèlement sur ses sites des systèmes de CA-DI-VS. Certes ambitieuse en raison notamment de l'effort financier qu'elle exige, cette opération doit être menée à son terme. Il faudra également prévoir le soutien puis le renouvellement des systèmes déployés.

Les modes d'actions de l'opération *Sentinelle* ont évolué dans le temps en fonction de la menace mais aussi et surtout en fonction de la prise en compte par les ministères des savoir-faire de chacun, avec le souci partagé d'une meilleure efficacité d'ensemble. Trois premières étapes ont été franchies : mise en place du dispositif composé de gardes statiques, ré-articulation du dispositif Île-de-France/province, transformation des gardes statiques en patrouilles. L'année 2017 doit consolider la quatrième étape qui doit aboutir à la définition d'effets à obtenir qui vont bien au-delà des « simples » patrouilles, permettant ainsi aux militaires d'opérer dans le cadre d'une mission et selon des modes d'actions identiques à ceux utilisés en opérations extérieures.

(24) *Hardware* construit par l'industriel, algorithme de chiffrement défini par la DGA et/ou l'industriel, clés de chiffrement élaborées par la défense.

(25) Exemple : système d'exploitation des réseaux informatiques.

À partir de la profusion de textes relatifs à l'intervention des armées sur le territoire national, fruit des réflexions de ces deux dernières années, l'État-major des armées (EMA) et le Commandement du territoire national (COMTN) récemment créé, s'emploieront à cette tâche en rédigeant un corpus doctrinaire qui inscrira dans la durée l'action de l'Armée de terre tous domaines confondus ⁽²⁶⁾, en cohérence avec les armées et les organismes qui concourent à la protection.

Sous commandement opérationnel du Chef d'état-major des armées (Céma), l'Armée de terre est engagée en permanence dans la fonction stratégique « protection » sur le sol national, aux côtés de l'Armée de l'air dans l'aérospatial et de la Marine nationale sur et sous l'eau. Ses résultats incontestables et incontestés depuis plus d'un quart de siècle ⁽²⁷⁾ justifient à eux seuls la présence des forces terrestres aux côtés de celles de sécurité intérieure. Pour autant, le dispositif *Vigipirate* – et dans une moindre mesure *Sentinelle* –, ne peut plus être considéré comme des dispositifs exceptionnels. Par ailleurs, les forces armées doivent être capables de poursuivre les opérations extérieures qui contribuent aussi à la protection de la Nation : elles doivent restaurer leurs moyens (humains, équipement) afin de renforcer leurs capacités opérationnelles. L'EMA et le COMTN auront à adapter le savant dosage interministériel qui optimise, dans l'espace et dans le temps, l'efficacité de chacune des contributions. Il pourrait se traduire par des réajustements intra et interministériels tout en sachant que le champ régalien, dans sa globalité, mérite des efforts.

Toujours dans le milieu terrestre, le Service de santé des armées (SSA) joue un rôle majeur, mondialement reconnu, dans le dispositif national de défense médicale contre les risques NRBC. Intervenant dans l'ensemble des fonctions du domaine, il pourrait se voir confier des responsabilités uniques dans le traitement *post-traumatiques* radiologiques et nucléaires.

Ainsi, les armées, directions et services sont désormais fortement sollicités dans la protection de la Nation. Leurs expertises et leurs moyens, autrefois plutôt utilisés en opérations extérieures, peuvent être avantageusement mis à contribution sur le territoire national.

La transformation digitale au service de l'approche globale de la fonction « protection »

Indissociables, interdépendantes et imbriquées les unes aux autres, les cinq postures nous invitent à éviter de raisonner avec des frontières et à appréhender davantage la protection dans sa globalité, dont la technologie numérique peut apporter sa plus-value.

La connectivité est réelle, qu'elle soit appréciée ou exécrée, acceptée ou refusée. Elle doit être vue comme une opportunité, celle de décroisser. Le « besoin d'en

(26) Espace/temps, planification et conduite, capacitaire (équipements, technologies, ressources humaines), légitimité, juridique.

(27) *Vigipirate* est un dispositif interministériel créé en 1978. Déclenché plusieurs fois depuis 1991 (guerre du Golfe), appliqué depuis 1996 (attentats du RER Port Royal) sans discontinuer. 2005 (attentats de Londres) est l'année à partir de laquelle il est resté au niveau rouge jusqu'à l'abandon du code couleur en 2014.

connaître » reste un levier incontournable pour préserver des intérêts, mais il peut aussi être un frein à l'efficacité collective. Le besoin de partager devient un devoir, ne serait-ce que pour la diffusion de signaux faibles. C'est pourquoi, il est judicieux de changer de paradigme, de passer d'une logique de « ne rien partager, sauf » à celle de « tout partager, sauf ». Il fera évoluer les mentalités, dans le sens d'un meilleur échange de l'information, même s'il reste à contrôler.

Plusieurs démarches concrètes peuvent être entreprises dans ce sens. Citons deux exemples. On pourrait envisager l'extension des réseaux informatiques de la défense dans les cellules de crise des préfectures, ce qui faciliterait la jonction défense-sécurité lors de la gestion d'événements pour lesquels les armées sont sollicitées. Une seconde piste serait de favoriser l'interopérabilité des SI entre acteurs du renseignement, ce qui constituerait une nouvelle étape importante après le rapprochement humain qui s'est intensifié dès 2015. L'exemple de l'organisation britannique peut être une source d'inspiration, étant donné son expérience dans le partage du renseignement. Cette organisation fédère et coordonne par le « haut » (niveaux politique et interministériel *via* le *National Security Council*) et par le « bas » (niveau inter-organismes *via* le *Joint Intelligence Committee*). A ainsi été constituée une communauté nationale unifiée du renseignement, dans le respect des prérogatives de chacun. Même s'il n'est pas nécessairement pertinent de chercher à transposer *ex-abrupto* le système britannique, son efficacité nous invite à renforcer le rôle du centre national du renseignement et à fédérer les SI du domaine à l'échelle du pays.

L'analyse des signaux faibles, qui concourt à la connaissance-anticipation, à la prévention, et *de facto* à la protection, repose fondamentalement sur les compétences et les ressources humaines. Les progrès technologiques particulièrement significatifs ces dernières années dans le domaine de l'analyse automatisée des données ⁽²⁸⁾ et de l'intelligence artificielle permettent d'envisager aujourd'hui, avec optimisme, de poursuivre le développement d'outils d'aide à la décision. Le « *Big Data* », avec tout ce qu'il implique dans sa définition (partage, gestion et analyse de l'information voix-données-images), constitue l'étape suivante dans laquelle la défense comme la sécurité doivent envisager leur transformation numérique. Afin d'établir le meilleur compromis entre libertés individuelles et sécurité collective, elles le feront en veillant scrupuleusement au respect de la législation amenée à évoluer en permanence dans ce domaine. Le résultat de la corrélation d'indices, calculée à partir du déclenchement d'une alerte d'origine humaine, peut faciliter le travail des autorités chargées de la protection du pays. Le « *Big Data* » peut en effet fournir à la communauté du renseignement une information issue du croisement d'informations ⁽²⁹⁾. Après avoir vérifié la pertinence des données et

(28) Lecture des plaques numérolologiques, reconnaissance physiologique (digitale, iris, faciale, etc.), traitement des langues, identification des mouvements, etc.

(29) L'exemple suivant permet d'illustrer la démarche dans son intégralité. Une alerte du départ brutal et inexplicé d'un jeune, dont le comportement laisse penser à une radicalisation, est donnée par des proches. Après récupération de photos d'identités, une présence est détectée en Syrie par un système de reconnaissance faciale, à partir d'images de combattants en Syrie provenant de systèmes d'observation spatiale militaires. Un système de reconnaissance faciale alerte son passage à la frontière française. La corrélation automatisée de ces données le catalogue comme « retournant ».

du calcul de corrélation, les responsables du premier cercle du renseignement du pays pourront décider ou non de diligenter une enquête.

En fait, les exemples concrets ne manquent pas. Le besoin accru de partage et d'interopérabilité est général. Intra et inter-milieus, intra et interministériels, intra et inter-États, il est d'ordre humain, organisationnel, procédural et... technologique. Dans la majorité des cas, la technologie numérique est en effet au cœur des enjeux.

Dans une approche prospective à dix ans, on peut considérer que le « *Cloud defense* » intégrera un nombre significatif d'équipements numériques présents sur les plateformes terrestres, aériennes et maritimes. Le « *Cloud defense* » dans sa complétude (univers spatio-cyber élargi à toutes ces plateformes) devra faire ainsi l'objet de toutes les attentions dans les études amont, car les technologies, encore immatures il y a une dizaine d'années, sont aujourd'hui prometteuses. Les technologies quantiques offriront des puissances de calcul inégalées. Les applications sont infinies, raison pour laquelle il est impérieux d'investir si l'on veut avoir l'ascendant. Dans le cadre de la fonction « protection », ces ruptures technologiques seront utilisées pour l'établissement de communications sécurisées ou pour la constitution d'ordinateurs ultra-puissants.

Conclusion

En définitive, il faut combiner avec une grande finesse les formidables atouts de la Nation pour la rendre plus résiliente. Les militaires doivent rester extraordinaires dans l'action, le temps et/ou l'espace. Cette alchimie passe par une ultra-connectivité informationnelle, organisationnelle et humaine, rendue possible par la plus-value fonctionnelle apportée par la technologie numérique, dont la puissance de calcul ne cesse d'augmenter exponentiellement. Cette connectivité est une réelle opportunité, sous réserve de bien la maîtriser ; le cas échéant, elle devient une vulnérabilité. Il convient également de bien la gouverner au quotidien car la préservation que demande l'État de droit constitue une exigence non négociable en démocratie. Ainsi, mise en œuvre et utilisée à bon escient, la transformation digitale peut aider à mettre sur pied une posture de protection globale et intégrée, sous le prisme défense-sécurité dont le continuum n'a jamais été aussi marqué. Elle démultipliera les effets des cinq postures de sûreté déjà fortement entrelacées : aérienne, maritime et terrestre d'une part, cyber et spatiale d'autre part.

Avant tout, chacune d'entre elles mérite d'être renforcée dans leur complétude à la hauteur des défis. Les efforts pour remplir cette mission régaliennne de protection doivent être au rendez-vous. Ils sont une exigence bien au-delà du ministère des Armées. Plus que jamais « l'affaire de tous », la défense et la sécurité doivent conduire à une profonde mutation de l'État-Nation. Le citoyen y a réellement toute sa place.

De la conduite et de la planification des opérations intérieures ⁽¹⁾

Stéphane MARCHENOIR

| Colonel (terre), auditeur de la 66^e session du CHEMA.

Le Chef d'état-major des armées (Céma) « assure le commandement militaire des opérations » ⁽²⁾. Ce commandement s'applique aussi bien sur les théâtres d'opérations extérieures que sur le territoire national. Hors domaine spécifique de la dissuasion, le Céma dispose du Centre de planification et de conduite des opérations (CPCO) pour planifier et conduire les opérations des armées. Cet outil performant a été créé en 2003 par la réunion du Centre d'opérations interarmées (COIA) – créé au début des années 1990 par l'amiral Lanxade pour qu'aucune opération à laquelle participent les forces françaises n'échappe à leur contrôle – et de l'État-major interarmées de planification opérationnelle (EMIA/PO). Il constitue la meilleure preuve de la capacité de réforme du ministère de la Défense (aujourd'hui des Armées). Confrontées à la guerre en opérations extérieures, les armées ont affirmé le primat de l'interarmées d'une part, et appris à se coordonner avec le ministère des Affaires étrangères et du Développement international (MAEDI) d'autre part.

Douze ans plus tard, en réaction aux attentats de janvier 2015, l'opération *Sentinelle* est déclenchée. Désormais en guerre ⁽³⁾ sur le territoire national, les armées interviennent massivement au sein d'une opération dont la responsabilité appartient au Minint. Elle répond parfaitement aux « effets à obtenir » définis par celui-ci et connaît en 2015 et en 2016 des évolutions mesurées et nécessaires. Toutefois, l'opération *Sentinelle* est aussi le révélateur des difficultés à conduire une opération militaire sous responsabilité Minint. D'un côté, il faut préserver la verticalité du commandement, gage d'efficacité de toute opération militaire. De l'autre, les crises au Minint se résolvent d'abord et avant tout à l'échelon du département ou de la zone de défense, dans une vision très horizontale et déconcentrée de la conduite des opérations. D'un côté,

(1) Formellement, il faudrait utiliser le terme de Mission intérieure (Missint) dont la définition est donnée dans la PIA 3-32-1, directive interarmées sur l'emploi de la force dans le cadre des missions intérieures, hors état d'exception (milieu terrestre) : « engagement sur le territoire national et sous le commandement du Céma en soutien, en accompagnement ou en complément de l'action civile de l'État dans les milieux terrestres, maritimes et aériens ». L'auteur privilégie dans ce document le terme d'Opération intérieure (Opint), par opposition à Opération extérieure (Opex), se basant sur une déclaration du ministre Jean-Yves LE DRIAN le 13 janvier 2015, parlant de l'opération *Vigipirate*, devenue *Sentinelle* par la suite : « C'est une opération militaire commandée par le chef d'état-major des armées. [...] C'est une opération militaire. Ce n'est pas de l'appoint. » Dans une acception plus générale, il faut comprendre le terme d'Opint comme « la contribution des armées à la défense non militaire », ne comprenant donc ni la Posture permanente de sûreté aérienne (PPS-A), ni la Posture permanente de sauvegarde maritime (PPS-M).

(2) Décret n° 2013-816 du 12 septembre 2013 relatif aux attributions du ministre de la Défense et du Céma.

(3) Discours du président de la République devant le Parlement réuni en Congrès, 16 novembre 2015.

les opérations se planifient dans une échelle de temps qui se compte en mois, avec la volonté de rechercher et prendre l'initiative ; de l'autre, elles se conduisent en réaction à l'événement la plupart du temps. Ce choc des cultures opérationnelles peut générer des tensions interministérielles, nées de suspensions et d'incompréhensions qu'il faut combattre.

Étudier l'origine du Centre des opérations des armées (COA), précurseur du COIA puis du CPCO permet d'en dégager quelques ressorts et invariants. Les confronter aux enseignements de l'opération *Sentinel* nous apprend que des marges de progrès existent dans la façon dont les armées conduisent et planifient la contribution des armées à la défense non militaire.

De l'origine du CPCO...

La genèse du CPCO est très directement liée à celle du poste de Céma. Pour ce dernier, en 1962, soit immédiatement après la guerre d'Algérie, une première étape est franchie puisqu'il hérite des responsabilités spécifiquement militaires au détriment du Chef d'état-major général de la défense nationale ⁽⁴⁾. Ceci n'a cependant pas d'effet immédiat sur la conduite des opérations militaires. Il faut attendre la réforme de l'EMA de 1976 et le début des engagements opérationnels français *post-guerres* coloniales pour que soit créé le Centre opérationnel des armées (COA). Il s'agit plus, à l'époque, de créer une cellule de veille continue qu'un centre de commandement et de contrôle. En effet, chaque armée reste alors responsable de ses engagements et possède un centre d'opérations (CO). Le COA fait exclusivement du suivi de situation grâce aux informations provenant des CO d'armées sur les opérations aéroterrestres conduites principalement au Tchad à l'époque. Les occasions de le faire évoluer vers des responsabilités opérationnelles plus importantes sont faibles. D'une part, il faut attendre 1982 pour que le Céma reçoive une autorité théorique à défaut d'être effective sur les chefs d'état-major d'armée, « lorsque des fonctions opérationnelles leur sont confiées » ⁽⁵⁾. D'autre part, les crises successives en Afrique des décennies 1970 et 1980 ne nécessiteront que l'envoi d'unités expéditionnaires des troupes de Marine ou de la Légion étrangère, avec l'appui de l'aviation, sans besoin de répondre à des actions d'envergure loin de leurs bases. L'immense majorité des armées est maintenue en retrait de l'Alliance atlantique face à la menace principale venant de l'Est.

La première guerre du Golfe fait prendre conscience au haut commandement militaire de la nécessité d'une évolution dans la conduite des opérations. L'amiral Lanxade est alors Chef d'état-major particulier (Cemp) à l'Élysée. Il constate certaines faiblesses dans l'organisation des armées. Il note en particulier que le Céma rencontre beaucoup de difficultés de coordination des actions militaires, largement conduites de façon autonome par les chefs d'état-major d'armées. Il en vient naturellement à penser que le Céma, compte tenu de sa compétence et de son expérience, doit être mis « à la

(4) « L'EMGDN redevient le SGDN, cédant ses responsabilités spécifiquement militaire à l'EMIA », Philippe VIAL, « La genèse du poste de Chef d'état-major des armées », *Revue historique des armées* n° 248, 2007.

(5) Décret n° 82-138 du 8 février 1982 fixant les attributions des chefs d'état-major.

place qui [lui] revient dans un processus de prise de décision politico-militaire adapté à la gestion des crises » ⁽⁶⁾, en accompagnement de méthodes politico-militaires de gestion des crises qui évoluent. Le ministère des Affaires étrangères (MAE) consulte progressivement davantage le ministère de la Défense, à l'imitation du président François Mitterrand qui, dès le déclenchement des hostilités, prend l'habitude de réunir chaque soir un conseil de guerre autour de son Céma et des chefs d'état-major d'armées. L'autorité militaire responsable de la conduite des opérations peut directement exprimer ses recommandations au chef des armées. « Le primat de l'interarmées se fait avec le retour de la guerre » ⁽⁷⁾. Une fois la guerre du Golfe terminée, seuls les Céma et CEMP participent aux conseils restreints.

Une nouvelle réforme de l'organisation opérationnelle des armées coïncide avec la nomination de l'amiral Lanxade comme Céma. Elle part de l'idée que la gestion des crises par les seuls cabinets appartient au passé. La méthode de gestion des conflits par les militaires eux-mêmes ayant fait ses preuves, il faut organiser la participation de ceux-ci aux instances qui traitent des opérations, à Paris au MAE et à l'étranger dans les organisations internationales telles que l'ONU, l'Otan et l'Union de l'Europe occidentale (EO). C'est la période où les armées prennent conscience qu'elles ne peuvent recevoir d'ordres que du Céma lui-même, par l'intermédiaire du Centre d'opérations interarmées (COIA), renommé pour souligner sa vocation interarmées. Ainsi, les militaires qui y servent, assument peu à peu le commandement et le contrôle opérationnel de toutes les opérations conduites par les armées françaises, permettant notamment de s'affranchir des interférences politiques mentionnées supra. Le COIA est ainsi structuré autour d'une cellule centrale et d'autant de cellules spécialisées que nécessaires. Celles-ci peuvent entrer en contact à tout instant avec le commandement militaire de chaque opération qui se déroule à des milliers de kilomètres. Ce lien est essentiel pour que ceux qui opèrent sur le terrain soient en phase avec le centre de décision politico-militaire de la capitale ⁽⁸⁾.

Arrêtons-nous un instant sur cette prise de pouvoir de la conduite des opérations par les militaires et soulignons combien l'amiral Lanxade et Pierre Joxe, alors ministre de la Défense, ont joué un rôle important dans cette dynamique. En 1988, l'amiral Lanxade sert au cabinet du Mindef et constate que les relations politico-militaires sont principalement traitées au sein du MAE où les militaires sont quasi-absents. Le peu de militaires présents est là « pour prendre acte des modes d'action retenus et transmettre les instructions aux états-majors » ⁽⁹⁾. Ce mode de fonctionnement le heurte à deux titres. D'une part, cela ne correspond pas à l'idée qu'il se fait du rôle du militaire dans la prise de décision politique dans la gestion d'une crise car qui peut « remonter » l'information opérationnelle vers le politique en lui donnant de précieuses interprétations sur le sens politique qui s'y rattache, sinon les soldats confrontés à la

(6) Jacques LANXADE, *Quand le monde a basculé*, NiL, 2001, p. 326.

(7) GA (2S) BENTÉGEAT, entretien.

(8) *Ibidem*, p. 330.

(9) *Ibidem*, p. 296.

complexité des terrains d'engagement ⁽¹⁰⁾ ? D'autre part, il estime que le cœur de la politique de défense est l'efficacité opérationnelle.

Ajoutons également que l'idée même de l'interarmées, qui repose sur la notion de synergie et d'efficacité opérationnelle, ne s'impose pas facilement. L'amiral Lanxade rencontre des oppositions fortes au sein des différentes armées à la mise en place de ses idées, en raison notamment des divisions entre les états-majors. Son opposition sur ce point avec le général Cot, commandant la 1^{re} Armée, est restée célèbre. Elle nécessite l'arbitrage de Pierre Joxe qui lui donne raison. Au sein de la Marine, les oppositions sont également très élevées, à l'image de celles existant entre les différentes catégories de forces navales. Le Céma met alors en œuvre une intuition, celle de saisir toutes les opportunités, visites dans les unités, conférences de presse, réunions, pour « parvenir à une véritable conduite interarmées des opérations » ⁽¹¹⁾. Ce faisant, il oblige ses opposants à s'exprimer et à débattre. Le discours peut pénétrer les esprits et le changement culturel s'opérer. Il faudra tout de même quatre années pour que cette transformation soit effective, avec l'aide d'opérations de plus en plus interarmées par nature.

L'échelon opératif prend également à cette période sa signification d'aujourd'hui. Il procède de la mise sur pied d'une chaîne opérationnelle complète, « dirigée depuis Paris par le COIA et placée sous l'autorité sur place d'un commandement de force disposant pour la première fois d'un PC interarmées constitué selon nos nouveaux concepts ». L'amiral Lanxade ajoute, s'agissant de l'opération *Turquoise* : « toutes les catégories de forces, notamment une composante aérienne de taille significative, [sont] intégrées dans cette nouvelle formule de poste de commandement qui a donné toute satisfaction. » ⁽¹²⁾. Pour la première fois, le lien entre une force interarmées et le Céma est établi au travers d'une chaîne de commandement complète et directe. La verticalité du commandement, concept sur lequel repose encore aujourd'hui toutes nos opérations, est établie.

Soulignons enfin que le COIA n'est pas le seul outil interarmées créé au début des années 1990. Citons par exemple le Commandement des opérations spéciales (COS), la Direction du renseignement militaire (DRM), l'État-major interarmées (EMIA) de Creil, le Collège interarmées de défense (CID), ainsi qu'au niveau ministériel la direction des affaires stratégiques. La fin de l'URSS et son corollaire le développement d'un monde multipolaire, accompagné du rôle majeur de la France dans la résolution de crises à l'étranger, en particulier en Afrique, se traduisent donc par une réforme en profondeur de l'organisation du commandement des armées.

Dix ans plus tard, au début des années 2000, les armées ont opéré leur mue d'une culture opérationnelle « guerre froide » vers une culture « opérations extérieures ». Elles sont alors confrontées au besoin de planifier les engagements au Kosovo et en Afghanistan, dans une approche plus intégrée que par le seul EMIA de Creil,

(10) Olivier ZAJEC, « Security studies et pensée stratégique française : de la vision globale à la myopie contextuelle » in *Res Militaris*, p. 13.

(11) *Op. cit.*, p. 326.

(12) *Ibidem*, p. 183.

lui-même travaillant sur un tempo inadapté à celui des opérations imprimé par le COIA. Avec la fusion du COIA et de l'EMIA/PO en 2003, le CPCO ainsi créé investit le champ de la planification froide, avec le souci de rester une structure réduite, pour ne surtout pas perdre en réactivité et en capacité de décision. Chaque bureau a donc son « satellite »⁽¹³⁾ : le J2, la direction du renseignement militaire ; le J3, les états-majors opérationnels d'armées ; le J4, le centre de soutien des opérations et des acheminements ; le J5, le commandement pour les opérations interarmées ; etc.

Pour paraphraser le général Castres⁽¹⁴⁾ et pour le résumer en 5 verbes, avec le CPCO, nous avons :

- « rapproché » les états-majors et les énergies autour des opérations ;
- « verticalisé » le commandement et le contrôle ;
- « partagé » l'information et l'appréciation de situation ;
- « anticipé », par le passage de la conduite à la planification ;
- « intégré » les avis, les apports et les ajouts des satellites du plus près au plus loin, comme ceux des missions militaires françaises par exemple.

Que faut-il en déduire ? Retenons principalement 3 idées :

- La confrontation à la guerre à l'extérieur a profondément modifié notre organisation militaire. Non seulement, le CPCO, aux ordres du Céma *via* le sous-chef opérations, permet de conduire les Opex avec agilité. Tout en délivrant la meilleure information possible, il assure également la puissance du Céma.

- Nul autre que les militaires peut mieux conseiller l'autorité politique sur la planification des opérations militaires. Citons combien le dialogue entre MAEDI/ASD⁽¹⁵⁾ et EMA/CPCO/J5 est fluide aujourd'hui. Nous pourrions faire la même observation avec nos instances internationales.

- La fin de la guerre froide semblait annoncer la fin de la menace sur le pays et ses intérêts. L'absence de confrontation à la guerre à l'intérieur a fait que jusqu'en 2015, la contribution des armées à la défense non militaire se limite au renfort ponctuel du Minint, essentiellement dans un volet sécurité civile des crises et en complément ponctuel des capacités de ce ministère.

Certes, en 1998, les armées participent à la sécurisation de la Coupe du monde de football dans une mission de sécurité intérieure. Mais elles restent « à côté » du Minint, pour reprendre une expression du général Delort⁽¹⁶⁾. Plus tard, la grande tempête de 1999 illustre assez bien la façon dont l'emploi des armées est conçu. Nous sommes quelques jours avant le réveillon de l'an 2000. Les armées se mettent à pied d'œuvre. L'idée maîtresse donnée par le ministre de la Défense est d'alimenter tous les foyers victimes de coupure électrique pour le réveillon. Tous les groupes électrogènes

(13) VA (2S) BADUEL, entretien.

(14) GA CASTRES, inspecteur général des armées (Terre), entretien.

(15) Affaires stratégiques de sécurité et du désarmement.

(16) Chef COIA de 1997 à 2000, entretien.

des armées sont sortis, 40 hélicoptères se mettent à disposition d'EDF pour remonter les lignes, la centrale de Blaye est sauvée par la réalisation de digues⁽¹⁷⁾. En communication, une seule question est sur toutes les lèvres : combien d'hommes les armées sont-elles capables de fournir ? Sans attendre leur déploiement effectif, le ministre annonce la mise sur pied de 6 000 militaires sur le terrain. Tout cela est commandé depuis la salle A33 du CPCO, déjà équipée par un concours de circonstance heureux en prévision du fameux *bug* de l'an 2000 ! Le temps politico-médiatique est le seul qui compte : une crise chasse l'autre.

Ce que révèle *Sentinelle* sur la conduite des opérations militaires intérieures

2015 est bien sûr l'année de la rupture. Jamais les armées, depuis le traumatisme de l'Algérie, n'avaient eu à s'engager aussi massivement sur notre territoire dans une mission de sécurité intérieure. Or, malgré des effectifs quatre fois plus faibles qu'à l'époque, les armées sont au rendez-vous. En effet, elles s'y préparent conformément à leur contrat opérationnel. Soulignons que l'intervention des armées sur le territoire national est non seulement prévue mais quantifiée dans le *Livre blanc de la Défense et de la Sécurité nationale* de 2013⁽¹⁸⁾. Bien des enseignements vont être tirés de cette crise. Retenons que la structure de l'organisation territoriale interarmées de défense, avec le CPCO à sa tête, a fourni le cadre indispensable au déploiement et à la mise en œuvre des 10 000 militaires engagés en trois jours.

L'opération *Sentinelle* est aussi le révélateur de l'immense défi pour les armées que représente un engagement sur le territoire national sous la responsabilité du Minint. Le premier d'entre eux est la différence de fonctionnement dans la résolution des crises : « le mode d'organisation centralisé des armées tranche avec la pratique déconcentrée de la sécurité intérieure »⁽¹⁹⁾. Le préfet de département est le véritable responsable de la sécurité dans son département et s'adresse bien souvent directement au ministre. Évidemment, il est jugé sur sa capacité à gérer ses problèmes de manière autonome, essentiellement avec ses moyens propres ou qui lui sont donnés en fonction des événements ayant lieu dans son département. Il dispose d'un interlocuteur militaire, le Délégué militaire du département (DMD), ne possédant quant à lui aucune capacité propre. Pour les obtenir, le DMD doit en effet s'adresser à l'officier général de zone de défense et de sécurité (OGZDS), autorité militaire placée en miroir du préfet de zone de défense et de sécurité (PZDS)⁽²⁰⁾, l'OGZDS devant lui-même les obtenir du CPCO⁽²¹⁾.

(17) GCA (2S) DELORT, entretien.

(18) « En cas de crise majeure, les armées apportent en renfort des forces de sécurité intérieure et de sécurité civile un concours qui pourra impliquer jusqu'à 10 000 hommes des forces terrestres, ainsi que des moyens adaptés des forces navales et aériennes ».

(19) Instruction du Minint relative aux modalités d'emploi des armées sur le territoire national n° 288/CAB/CR/GD du 12 juillet 2016, p. 4.

(20) « Responsable de la préparation et de l'exécution des mesures de sécurité nationale au sein de la zone de défense et de sécurité » et « responsable de la coordination avec les autorités militaires des mesures de défense et de sécurité nationale ». Article R122-4 du code de la sécurité intérieure.

(21) « Le Céma exerce, sans jamais le déléguer, le commandement opérationnel (OPCOM) des engagements militaires », doctrine d'emploi des forces, DIA-01(A)_DEF(2014) n° 128/DEF/CICDE/NP du 12 juin 2014.

Le second défi, loin derrière le premier, vient de ce que l'organisation du Minint, lorsqu'elle a besoin de faire appel aux armées, est plus particulièrement adaptée à la gestion de crises de sécurité civile ⁽²²⁾. L'interlocuteur de l'État-major de zone de défense (EMZD) ou de l'État-major interarmées de zone de défense et de sécurité (EMIAZDS) ⁽²³⁾ est l'État-major interministériel de zone (EMIZ), peu fourni en gendarmes et policiers, *a contrario* des pompiers. Le plan gouvernemental *Vigipirate* ⁽²⁴⁾ existe mais ne représente pas un enjeu pour les armées avant janvier 2015 dans la mesure où les effectifs précédemment déployés sont faibles ⁽²⁵⁾.

Même dans la façon d'appréhender le problème, les réflexes sont différents. Les uns comptent leurs troupes en nombre d'Unités de force mobile (UFM), les autres veulent des effets à obtenir ; les uns revendiquent « l'allocation de la ressource entre les zones », les autres veulent garder la responsabilité de l'adéquation du volume de forces à la mission ; les uns gèrent des « exigences politiques impératives » ⁽²⁶⁾, les autres veulent garder la main sur le mode d'action employé.

Les mesures prises

De la même façon que le MAE dictait les modes d'action aux militaires avant que ces derniers ne conseillent au plus près les plus hautes autorités politiques du pays comme évoqué supra, le Minint et les autorités administratives régionales commencent par employer les militaires comme des vigiles pendant de longs mois. Ce point ayant été largement commenté, soulignons simplement qu'il faut attendre l'attentat terroriste du 14 juillet 2016 à Nice pour que soient prises trois mesures importantes à l'issue de l'été : répartition à 50/50 entre Paris et province, modes d'action entièrement dynamiques, et niveau d'engagement revenu à 7 000 militaires. Il faut dire que depuis janvier 2015, les structures de dialogue interministérielles se sont mises progressivement en place. Les cabinets ministériels se rencontrent régulièrement, le CPCO et le haut fonctionnaire de défense et de sécurité du Minint également par le biais de la Cellule de coordination Intérieur-Défense (C2ID), et le dialogue zonal est facilité par la mise en œuvre de plusieurs directives.

Toutefois, des progrès doivent encore être faits en s'appuyant sur l'expérience des opérations extérieures.

Quelles conclusions pour les armées ?

Compte tenu des différences profondes, dans les organisations et dans les cultures, il n'y a pas de changement rapide, ni majeur à prévoir, hors décision *post*-électorale qui viendrait remettre en cause la nature de l'engagement actuel. Même s'il

(22) Note DPPSN/HFDA du 28 juillet 2011 sur la répartition des compétences entre la Direction générale de la sécurité civile et de la gestion des crises (DGSCGC) et le Service du haut fonctionnaire de défense (SHFD).

(23) Lille et Marseille sont des EMIAZDS. Paris, Lyon, Rennes, Bordeaux et Metz sont des EMZDS.

(24) *Vigilance et protection des installations contre les risques d'attentat terroriste à l'explosif*.

(25) Inférieurs en moyenne à 1 000 militaires.

(26) *Op. cit.*, p. 10.

ne faut surtout pas dénigrer les mesures prises à l'été 2016 décrites *supra*, gardons à l'esprit certaines vérités.

La première d'entre elles est celle de l'efficacité. Elle intéresse autant le militaire qu'elle n'est pas la priorité du politique, malgré ce qu'il affirme ⁽²⁷⁾. L'efficacité de l'emploi des militaires pour le politique réside dans l'effet d'annonce. Les armées rassurent, sont visibles et tant mieux si elles sont dissuasives. Cela ne doit pas les empêcher de rechercher chaque occasion pour améliorer leur efficacité, tout en ayant conscience que ce n'est pas le seul critère de l'équation. En revanche, gare au discrédit. Rien ne leur sera pardonné.

La deuxième est que nous sommes engagés pour longtemps dans des missions de sécurité intérieure. Il n'est pas certain que les élections présidentielles de 2017 conduisent à une remise en question de l'opération *Sentinelle*. De la même façon que les opérations extérieures ont transformé notre haut commandement opérationnel militaire, sachons nous réformer pour garantir le même niveau professionnel s'agissant des opérations intérieures. Cela nécessite de redéfinir un cadre clair et de dresser des perspectives sur de nouvelles formes d'engagement sur le territoire national. À titre d'exemple, le travail de réflexion actuel pour rendre nos postures plus agiles, plus réactives et mieux cadencées, participe de la définition d'un « faire autrement » sur le territoire national.

À la différence des PPS Air et Marine, où les armées s'engagent sous l'autorité du Premier ministre, dans le milieu terrestre les armées sont placées sous la responsabilité du ministre de l'Intérieur. C'est d'emblée moins facile même si le commandement opérationnel du Céma sur les opérations intérieures est parfaitement compris. Adoptons résolument la posture opérationnelle de ministère « concourant » du Minint pour la contribution des armées à la défense non militaire en intervenant au juste niveau pour des missions pour lesquelles nous avons une plus-value et en préservant la verticalité du commandement.

Les solutions à mettre en œuvre

Rechercher l'efficacité

Le premier facteur d'efficacité dans le commandement des Opint, hors PPS Air et Marine, est le même que pour celui des opérations extérieures, à savoir la verticalité du commandement des opérations. Ceci permet au Céma d'exercer l'OPCOM et donc de s'assurer du meilleur emploi de ses militaires. Accessoirement, c'est aussi grâce à cette verticalité qu'il assoit sa crédibilité dans ses relations politico-militaires. Rien ne doit donc affaiblir cette verticalité, ni l'organisation du soutien, ni celle des opérations. Pour cette dernière, le CPCO ne peut jamais être mis devant le fait accompli. Le dialogue civilo-militaire des niveaux départemental et zonal doit se faire selon le principe de subsidiarité, à la condition qu'aucune décision de ce niveau n'impacte la cohérence d'ensemble de la mission intérieure quelle qu'elle soit. Ainsi, avant

(27) GA(2S) BENTÉGEAT, entretien.

toute signature de réquisition administrative, l'avis du Céma, *via* le CPCO, doit être recherché.

Toutes les occasions de conseiller l'autorité administrative ou politique sur l'emploi des militaires doivent être saisies. Cela nécessite un investissement humain dans toutes les instances de décision du Minint, ainsi que dans toutes les cellules de crise. Tant que le Minint n'aura pas rationalisé ses structures de commandement, les armées doivent se préparer à déployer des détachements de liaison dans chacune des strates de décision de ce ministère, en veillant à ne pas affaiblir le niveau d'expertise du Céma. Ne pas le faire conduirait à s'exposer à des décisions unilatérales pouvant nuire à l'efficacité opérationnelle.

Enfin, pour augmenter l'efficacité de l'engagement des armées, il faut faire effort sur le niveau tactique pour que les militaires sachent intervenir en complément des forces de police et de gendarmerie en cas de coup dur, et inversement. Cela passe par un référentiel interministériel bien partagé, des exercices communs et des doctrines d'emploi mieux définies. Ne pas le faire peut conduire à la disqualification.

Les opérations intérieures font partie désormais du patrimoine génétique des armées

Nous avons souvent répété que notre engagement *ici* ne devait pas remettre en question notre aptitude à gagner en opérations *là-bas*. Une autre façon de le dire est la suivante : ne pas affaiblir ce que nous sommes les seuls à pouvoir faire, à savoir mener des opérations extérieures. Or, le problème ne se pose plus exactement en ces termes. Nous sommes engagés sur notre sol probablement pour longtemps. C'est donc, après le temps de la guerre froide et celui des opérations extérieures, celui d'un engagement en opération intérieure devenu prépondérant. Cela appelle un changement culturel. Il faut que nous communiquions davantage sur cet engagement pour qu'à la manière d'un amiral Lanxade appelant à ce que s'expriment les oppositions à l'interarmées pour mieux les contrer, les oppositions à l'interministériel puissent petit à petit devenir minoritaires. Bien-sûr sans oublier que le soldat de l'intérieur est aussi le soldat de l'extérieur !

Le dire est une chose, le faire en est une autre. Passons de la théorie à la pratique. Développons un vivier d'hommes et de femmes rompus à l'interministériel. La réussite des opérations récentes est en très large partie due à la qualité des hommes qui servent dans la chaîne des opérations. C'est aussi parce que les chefs se connaissent que les décisions du niveau central peuvent être prises avec l'éclairage des chefs opératifs et tactiques. Il en est évidemment de même pour les opérations intérieures. Cultivons un vivier de militaires qui connaissent aussi bien le Minint que les opérations. Cet investissement permettra la confiance mutuelle et le succès en opérations. Accompagnons-le de propositions pour acculturer nos hommes politiques et nos autorités administratives aux armées : stages au sein des écoles de formation, séminaires, interventions de nos détachements de liaisons (DL), développement d'outils de communication, etc.

Enfin, admettons que le Minint puisse planifier et conduire les opérations de façon différente de celle des armées, *a minima* selon un tempo différent. Cherchons

à comprendre comment les UFM s'entraînent, comment elles sont générées, comment leur engagement est planifié et comment les capacités des armées peuvent s'inscrire en complémentarité de celles du Minint. Attachons-nous à bien connaître leur référentiel : périmètre géographique du département contre celui de la zone de défense, déconcentration des responsabilités contre commandement centralisé, logique de moyens contre logique d'effet, etc. De notre côté, connaissons parfaitement les règles d'engagement des armées sur le territoire national, pour que chacun applique son niveau de responsabilité. Le traumatisme de la grotte d'Ouvéa doit être enseigné ⁽²⁸⁾.

Sachons aussi ne pas aller trop loin pour ne pas transformer tout ou partie de nos armées en force de sécurité publique. Cela passe par des réponses claires aux questions suivantes : jusqu'où s'engager sur le territoire national ? Quelle est la nature de notre adversaire ? Avons-nous un ennemi ? Doit-on rechercher plus d'autonomie ? Quelles limites aux équipements spécifiques ? En faut-il ?

Être un allié fiable dans une coalition antiterroriste sur le territoire national

Agir en qualité de « concourant » dans une coalition impose de ne faire aucune concession. En allié fiable, osons dire les choses.

Rappelons que c'est parce que l'amiral Lanxade était CEMP, suffisamment proche du pouvoir mais pas encore en responsabilité, qu'il a su identifier les leviers d'amélioration de l'organisation du haut commandement militaire. Lorsqu'il a été désigné Céma, ayant la totale confiance de son chef, il a pu mettre en application ses idées. Les armées peuvent désormais jouer ce rôle vis-à-vis du Minint. Ayant réussi à créer l'interarmées pour « gagner en opérations » à partir de forces armées très indépendantes, elles peuvent théoriser ce succès pour que le Minint s'en inspire pour adapter son organisation interservices et interdirections générales.

À ce titre, le CPCO est sans doute un modèle à regarder de près pour en créer un au sein du Minint ⁽²⁹⁾. Il s'agit d'un outil de commandement et de contrôle à la fois suffisamment petit pour garder sa capacité à proposer des décisions en temps contraint, et suffisamment connecté avec ses satellites pour qu'ils puissent apporter leurs propres idées sur les opérations qu'ils suivent par ailleurs de très près. Balard a commencé à produire des effets. En regroupant les entités du ministère autour du « réacteur nucléaire » des opérations, les armées continuent d'améliorer l'outil.

De même, nos engagements en Opex nous apprennent que la lutte contre le terrorisme passe par une approche inclusive et décloisonnée. C'est en s'intéressant aux filières économiques et financières des réseaux d'approvisionnement d'armes et de munitions que les armées obtiennent leurs meilleurs résultats dans la lutte contre les

(28) Après le massacre de 4 gendarmes de la brigade de Fayaoué, dans l'île d'Ouvéa, en Nouvelle-Calédonie, 27 gendarmes sont pris en otages et conduits dans une grotte. Le général commandant supérieur des forces armées est chargé seul et informellement de s'engager dans une opération de libération d'otage, sans que les autorités civiles responsables soient formellement impliquées dans le processus de décision. Cet engagement hors cadre légal dans une opération de maintien de l'ordre, où deux militaires perdront la vie, sera judiciairement reproché aux autorités militaires, même si une amnistie générale mettra un terme aux procédures pénales.

(29) Pour son propre bénéfice et dans la limite de ce que nos progrès puissent être transposables.

engins explosifs improvisés. C'est en partageant le renseignement que les armées ont réussi à planifier des opérations en coalition. Si la prise de conscience du caractère transverse de la menace est réelle, il est sans doute possible d'aller plus loin dans la façon dont les informations sont échangées. Les armées doivent bénéficier des informations du Minint, dans la limite du besoin d'en connaître, car le territoire national est désormais un théâtre d'engagement à part entière.

Conclusion

L'origine du CPCO offre un bel exemple de la faculté d'adaptation des armées confrontées au retour de la guerre « à l'extérieur ». Elles en ont fait un outil performant, qui a également permis, jusqu'en 2015, de planifier et conduire des missions d'appui aux unités de la sécurité civile du Minint.

Confrontées au retour de la guerre « à l'intérieur », la nature de leur engagement se recentre sur des opérations de sécurité intérieure, pour lesquelles elles demeurent des forces concourantes du Minint. Dès lors, l'efficacité de leur engagement passe par une capacité à participer à la conception des opérations sur le territoire national. Elles sauront le faire si elles agissent en coalition avec le Minint.

Connaissant la guerre à l'extérieur, menée en coalition, elles doivent apporter toute l'expertise des opérations au Minint. Cela nécessite un effort en ressources humaines pour mieux connaître le Minint, un effort doctrinal pour transposer nos acquis en Opex en inspirations pour le territoire national, ainsi qu'une relation de confiance avec un ministère qui a beaucoup à gagner à se rapprocher des armées. À celles-ci de faire preuve de toute la pédagogie nécessaire, tant au sein de ses organisations qu'au sein du Minint. Ainsi pouvons-nous imaginer le Mindef aussi bien connecté avec le Minint s'agissant des opérations intérieures qu'il l'est avec le MAEDI s'agissant des opérations extérieures.

De la conduite et de la planification des opérations intérieures

Éléments de bibliographie

Livre blanc de la Défense et de la Sécurité nationale, La Documentation française, 2013, 160 pages.

Code de la sécurité intérieure (www.legifrance.gouv.fr/).

Discours de François HOLLANDE, président de la République devant le Parlement réuni en Congrès, 16 novembre 2015 (www.assemblee-nationale.fr/14/cri/congres/20154001.asp).

Articles de loi

- Décret n° 2013-816 du 12 septembre 2013 relatif aux attributions du ministre de la Défense et du Céma.
- Décret n° 82-138 du 8 février 1982 fixant les attributions des chefs d'état-major.

Instructions

- Instruction du Minint relative aux modalités d'emploi des armées sur le territoire national n° 288/CAB/CR/GD du 12 juillet 2016.

Documents de doctrine

- Doctrine d'emploi des forces, DIA-01(A)_DEF(2014) n° 128/DEF/CICDE/NP du 12 juin 2014.

Articles

VIAL Philippe, « La genèse du poste de Chef d'état-major des armées », *Revue historique des armées* n° 248, 2007.

ZAJEC Olivier, « *Security studies* et pensée stratégique française : de la vision globale à la myopie contextuelle » in *Res Militaris*, p. 13.

Littérature

LANXADE Jacques, *Quand le monde a basculé*, NiL, 2001, 400 pages.

Entretiens

- Général d'armée (2S) Henri BENTÉGEAT, ancien Céma.
- Général d'armée Didier CASTRES, inspecteur général des armées (Terre).
- Général de corps d'armée (2S) Dominique DELORT.
- Vice-amiral d'escadre (2S) Patrick HÉBRARD.
- Vice-amiral (2S) Franck BADUEL, ancien chef du CPCO.
- Général de brigade Thierry BURKHARD, chef conduite du CPCO.
- Général de brigade NICOL, COMTN de l'AdT (Commandant territoire national de l'Armée de terre).
- Colonel Pierre LAURENT, chargé d'anticipation synthèse territoire national au CPCO.

Avant-postes de forces légères

Laurent CLUZEL

| Colonel (terre), auditeur de la 66^e session du CHEM.

« Quel est le but de notre cavalerie légère en campagne ? D'éclairer et protéger la marche de notre armée. Comment est atteint ce but ? En avançant nos colonnes ; éclairant leurs flancs, les entourant et couvrant d'un rideau vigilant et courageux ; suivant l'ennemi pas à pas, l'inquiétant, éventant ses projets, épuisant ses forces en détail, détruisant ses magasins, enlevant ses convois et le forçant enfin à dépenser en défensive la puissance offensive dont autrement il aurait tiré ses plus grands avantages ⁽¹⁾. » Par ces lignes écrites en 1831, le colonel de Brack introduisait ses fameux *Avant-postes de cavalerie légère*, livrant la quintessence de son expérience guerrière acquise dans l'éclat des campagnes impériales et mûrie dans l'obscurité du temps de paix.

Ses mots ne sont pas sans écho dans la mémoire immédiate de nos opérations extérieures. Face à la double menace du radicalisme islamiste, qui survivra à la défaite de *Daech*, et des États-puissances, dont les stratégies se dessinent aujourd'hui, ils s'accordent surtout avec l'enseignement militaire majeur ⁽²⁾ des conflits récents : la nécessité d'inverser le principe d'incertitude, en le faisant peser sur l'adversaire. À l'horizon de 2030, une constellation d'avant-postes de forces légères, multidimensionnelles et intégrées pourrait garantir la réactivité de nos armées, la permanence de notre dispositif de veille, l'ubiquité de nos forces en dépit de l'immensité, l'autonomie des éléments engagés et la foudroyance de notre action dès lors que l'ennemi se révèle.

- Comment constituer ces avant-postes, non seulement dans les champs aéroterrestres et aéromaritimes, mais aussi dans ceux de l'immatériel – espace, cyberspace et perceptions ?
- Comment préparer les troupes, les chefs et leurs états-majors à les armer ?
- Comment garantir le souffle opérationnel des armées à cet effet ?

Telles sont les questions auxquelles cette étude tentera de répondre en exploitant la richesse des conférences données au Centre des hautes études militaires (CHEM) et à l'Institut des hautes études de défense nationale (IHEDN), en analysant les documents prospectifs des armées et en puisant tant dans l'expérience opérationnelle récente que dans la littérature inspirant de longue date l'exercice du métier des armes.

(1) Antoine-Fortuné DE BRACK, *Avant-postes de cavalerie légère*, Carrefour du net Éditions, 2011 (réédition), p. 43.

(2) Étude du COMITÉ D de la 66^e session du CHEM, *Leçons à tirer des conflits récents*, décembre 2016.

Veiller sur le nouveau limes : « l'hiver vient... »⁽³⁾

Comment comprendre la notion d'avant-postes ?

Avant-postes de forces légères, sentinelles de l'immensité. Ou le soldat face au défi de l'ennemi, dans une double dimension, celle du temps et de l'espace.

La notion d'avant-poste prend la plénitude de son sens lorsqu'existent des « colonnes », efficaces à condition d'être puissantes, mobiles, résilientes et connectées à ces avant-postes. Ceux-ci se définissent alors comme « des éléments armés placés en avant du gros des troupes »⁽⁴⁾. Mais à la différence des sentinelles, les avant-postes peuvent engager le combat, doivent même être capables de le faire, ce qui suppose une organisation, des équipements et des forces morales *ad hoc*. Leur capacité à dissuader l'ennemi procède pour beaucoup de cette agressivité potentielle. De fait, ce sont les « postes placés le plus près de l'ennemi », selon la définition du dictionnaire *Litttré*, ou encore les « postes détachés en avant d'une place, d'un corps de troupes, pour surveiller l'ennemi et prévenir ses attaques »⁽⁵⁾. Au sens figuré, ils représentent « tout ce qui sert de défense avancée contre un ennemi extérieur ». Car la fonction des avant-postes n'est pas seulement de surveiller, de prendre et préciser le contact, mais aussi, le cas échéant, de décourager l'ennemi en montrant des crocs d'autant plus acérés qu'ils seront perçus comme un avant-goût d'une mâchoire plus redoutable. On tombe alors dans la dialectique entre avant-poste et gros de la troupe. Du reste, en notre époque de grandes ruptures temporelles – écrasement des temps politique et médiatique, et donc des délais de réaction – et spatiales – paradoxe des frontières clamées, revendiquées, transgressées ou contournées – existe-t-il encore une différence entre avant-poste et avant-garde⁽⁶⁾ ? Le terme d'avant-poste pourrait suggérer une approche statique, immédiatement balayée par les propos introductifs du colonel de Brack : les avant-postes doivent être mobiles.

Les avant-postes sont-ils uniquement militaires ? À tout le moins, les services de contre-espionnage en font partie au premier chef. Mais sans doute convient-il d'adopter une démarche encore plus large à leur égard... Sont-ils uniquement humains ? De toute évidence, non, la technologie constituant un facteur de supériorité lorsqu'elle est maîtrisée. Pour autant, la dimension humaine demeure au cœur des avant-postes : c'est bien la volonté de vaincre qui donne un sens au dispositif de défense, dont les avant-postes ne sont qu'une composante. D'ailleurs, le colonel de Brack décrit des colonnes en marche, c'est-à-dire se dirigeant vers un but, vers des objectifs à atteindre dans le cadre d'une stratégie. Comme le souligne le bon sens cavalier, *un char immobile est un char détruit...* La notion d'avant-poste s'avère ainsi utile pour stimuler

(3) Devise de la Maison Stark, suzerain inféodé du Trône de Fer pour les contrées du Nord, dans la série télévisée américaine (HBO) *Game of Thrones*, adaptée à partir de 2011 des romans de R.R. MARTIN. C'est aussi le titre du 1^{er} épisode qui s'ouvre sur 3 patrouilleurs de la Garde de Nuit (apartisans) en mission par-delà le Mur, barrière massive de glace séparant le Royaume, des terres sauvages à son extrême Nord, comme un rappel romancé de l'antique mur d'Hadrien.

(4) Définition volontairement tirée du *Wiktionnaire*, dictionnaire en ligne (<https://fr.m.wiktionary.org/wiki/avant-poste>) et donc peut-être l'un des plus communément et immédiatement accessibles aujourd'hui.

(5) Définition du centre national de ressources textuelles et lexicales (CNRTL), créé par le centre national de la recherche scientifique (CNRS) pour fédérer un ensemble de ressources linguistiques et d'outils de traitement de la langue (www.cnrtl.fr/definition/avant-poste).

(6) Carl VON CLAUSEWITZ, *De la guerre* (Éditions de Minuit, 2005) et plus précisément le livre V, chapitre VII : « Avant-garde et avant-postes ».

un esprit de défense qui ne doit pas se rassurer dans l'épaisseur des murailles de la cité mais au contraire se porter toujours en avant, à la frontière, sur le rift, pour voir, comprendre, anticiper.

Mettre en exergue la notion d'avant-postes de forces légères présente donc l'intérêt de faire prendre conscience à toute la Nation du danger qui la menace. Sentinelle sur le rempart, garde de nuit patrouillant au-delà du *limes*... Personne n'y croit, jusqu'au grand fracas.

Les avant-postes doivent nous garder toujours en mouvement, en éveil, en vigilance.

Mais laissons pour l'heure ces considérations théoriques pour oser l'effort de vision prospective.

Dans dix ans, où et face à qui déployer nos avant-postes ?

Projetons-nous en l'an 2027, au-delà des deux prochains quinquennats présidentiels et des enjeux de la loi de programmation militaire... Bien malin celui qui pourrait décrire avec certitude l'état du monde à cet horizon, alors même que notre futur immédiat s'avère plus imprévisible que jamais, comme le soulignent par exemple les inquiétudes sécuritaires des pays de l'Otan à l'approche du Sommet de l'Alliance Atlantique ⁽⁷⁾, le pessimisme politique du chef de la Commission européenne ⁽⁸⁾, voire l'alarmisme sanitaire de Bill Gates ⁽⁹⁾. Tentons toutefois, pour la France, de dégager sinon la moindre certitude, du moins quelques grandes lignes stratégiques rapportées à la tectonique des plaques impériales telle qu'on peut la discerner aujourd'hui.

Le monde occidental restera durablement harcelé de l'extérieur et ébranlé de l'intérieur.

Avec une agressivité de plus en plus ostensible, les Russes testent la fiabilité de notre système de défense et de réaction, depuis les confins de l'Arctique jusqu'à la péninsule ibérique. Ils avancent leurs pions en Europe centrale, suscitant l'inquiétude des pays de l'ancien empire soviétique, annexant les territoires qu'ils estiment vitaux, à l'instar de la Crimée, convoitée et disputée depuis le règne de Catherine II. Face à cette démonstration de retour en puissance, la France doit non seulement protéger ses approches aériennes et maritimes, mais aussi garantir sa solidarité vis-à-vis de ses alliés européens – les Britanniques notamment, quoiqu'il advienne du *Brexit*. Dans le même temps, il lui faut devenir plus dissuasive, voire offensive, dans le nouveau champ de bataille du cyberspace, si outrageusement mais efficacement razziié par les *negative influencers* de Moscou.

Nos avant-postes se situeront le long des lignes de fracture de puissance ; l'influence russe tous azimuts n'en sera pas la moindre dans les dix ans à venir.

(7) « Le chef du Pentagone s'emploie à rassurer ses partenaires de l'Otan », *France24.com*, 15 février 2017.

(8) « L'UE évolue dans des directions différentes selon les pays, des directions difficilement compatibles entre elles », propos tenus par Jean-Claude JUNCKER sur la radio allemande *Deutschlandfunk*, à quelques semaines de l'ouverture des négociations sur le *Brexit*, *Le Monde.fr*, 12 février 2017.

(9) « Nous nous mettons en danger en ignorant le lien entre sécurité sanitaire et sécurité internationale » : lors de la conférence de sécurité de Munich, le milliardaire a jugé « probable » une catastrophe mondiale émanant « de la nature ou des terroristes », *Le Point.fr*, 18 février 2017.

Le cyberspace n'est du reste pas investi par les seuls cosaques numériques de l'empire des steppes. D'autres puissances s'y déploient, sans doute plus silencieusement mais plus sûrement, selon un autre rapport au temps. L'Empire du Milieu n'a certainement pas délaissé le champ des perceptions. La Chine semble en effet étendre inexorablement son influence sur la planète, à l'instar des îlots perdus qu'elle transforme magistralement dans l'océan Pacifique en autant de points d'appui de sa puissance, véritables bases de contrôle des immenses espaces maritimes sur lesquels elle impose sa souveraineté. Si l'on peut voir là un vrai défi stratégique pour les États-Unis naturellement orientés vers le Pacifique – souvenons-nous de la reconquête terriblement opiniâtre par les *Marines* des îles aux mains des Japonais durant la Seconde Guerre mondiale – il serait malheureux de négliger notre propre rôle dans cet espace où les Français s'avèrent assurer la dernière présence militaire européenne permanente.

Nos avant-postes s'envisageront à l'échelle de la planète, selon toutes les dimensions physiques, morales, spatiales, informationnelles et numériques.

La Chine ne se contente d'ailleurs pas du développement de son influence en Asie et dans le Pacifique. Elle va massivement chercher ses ressources en Afrique, côtoyant, pour l'heure, nos forces déployées ou prépositionnées, comme dans l'État – garnison internationale – de Djibouti ⁽¹⁰⁾. De fait, la Chine se montre partout où ses intérêts lui dictent de disposer d'atouts de puissance : points de passage obligé des routes commerciales maritimes, points de convergence ou de concentration des câbles numériques, *hubs* terrestres, aériens et numériques continentaux... Cette empreinte durable dans notre ancien empire mérite d'être intégrée comme une donnée majeure à la fois pour la préservation de notre propre influence, mais aussi comme une possibilité d'interaction lucide ⁽¹¹⁾, face au redoutable défi de contrôle des circuits d'échanges transafricains, du golfe de Guinée à la Méditerranée et au Moyen-Orient en passant par la vaste Bande sahélo-saharienne (BSS). Ces axes autrefois sillonnés par les grandes caravanes se trouvent au cœur des trafics d'armes, de drogue et d'êtres humains ⁽¹²⁾. Enjeux de liberté d'action pour les organisations terroristes, ils permettent la jonction physique entre l'espace sahélien et le Levant avec des débouchés, d'une part au Nord, sur l'Europe *via* la Maghreb déstabilisé par les printemps arabes et le chaos libyen ; et d'autre part au Sud, vers le centre de ce continent que les pessimistes estiment au bord de l'implosion. Il apparaîtrait primordial d'agir dans cet espace comme aux avant-postes de notre propre territoire. C'est ce à quoi la force *Barkhane* s'emploie en intensifiant la coopération opérationnelle avec les pays du G5 Sahel (Mauritanie, Mali, Burkina Faso, Niger et Tchad) ; c'est ce que la France continuera d'assurer pendant au moins dix ans, en position menante puis – le plus rapidement possible – concourante, en élargissant le champ de son action partenariale et en stimulant sa mémoire ⁽¹³⁾.

(10) Outre les forces françaises présentes depuis 1862, Djibouti compte déjà dans l'espace limité de son territoire une base américaine de 5 000 hommes implantée en 2002, dans le sillage des attentats du 11 septembre 2001, et une base japonaise de 1 000 hommes. L'Arabie saoudite souhaite s'y installer et la Chine va y déployer sa première base extérieure qui pourrait accueillir jusqu'à 10 000 hommes.

(11) « L'avenir de Djibouti s'écrit avec la Chine », Anne BAUER, *Les Echos*, 1^{er} mars 2017.

(12) Voir à ce sujet l'excellente infographie de Flavie HOLZINGER et Jules GRANDIN : « Tout comprendre à la poudrière du Sahel en cartes » *Le Monde.fr*, 4 février 2017.

(13) Cf. Carte de l'emplacement des troupes de l'Afrique occidentale française (AOF) au 31 juillet 1914, archives de la bibliothèque du 11^e Régiment d'artillerie de Marine.

Nos avant-postes tiendront la ligne de notre histoire qu'il importe d'apaiser ; ils seront armés en partenariat avec ceux qui l'ont écrite à nos côtés.

De fait, agir sur cette ligne de Dakar à Djibouti, c'est veiller sur les mouvements vers la Méditerranée, limiter la pression migratoire, circonscrire l'action terroriste dans des espaces distincts où elle peut être détruite, rester prêt à réagir de part et d'autre de la Grande Bleue en cas de détérioration brutale de la situation dans le pays le plus préoccupant pour la décennie à venir – l'Algérie – et donner un gage de puissance et de solidarité à notre allié le plus puissant mais aussi, depuis peu, le plus imprévisible – les États-Unis. Ceux-ci demeurent naturellement menants dans les actions de la coalition au Moyen-Orient et ont vocation à le rester, tant que *Daech* n'aura pas été militairement vaincu en Irak. Mais leur position dans le complexe conflit syrien s'avère fragile. D'autres stratégies de puissance y sont de nouveau en œuvre, entre trois vieux empires – perse, russe et ottoman. Identifié par les Américains dans l'« axe du Mal », l'Iran réintègre progressivement le jeu diplomatique ; membre ancien de l'Alliance Atlantique, la Turquie inquiète et fragilise aujourd'hui sa cohésion. La lucidité s'impose donc dans la gestion sinon dans la résolution d'un véritable système de crises : notre intérêt prime, dans le respect de nos valeurs ; nos alliances s'articulent et se réarticulent autour, en fonction de nos besoins.

Nos avant-postes pourront intégrer ou s'intégrer ; leur constellation couvrira « d'un rideau vigilant et courageux » le paysage évolutif des sphères d'influence.

Enfin, sur notre propre territoire hexagonal et ultramarin, comment pourrions-nous négliger les tout premiers avant-postes, alors même que les menaces extérieures et intérieures continueront de s'alimenter l'une de l'autre ? À cet égard, nous avons clairement changé de monde : la menace est également chez nous ; la combattre inlassablement impose de réviser les lignes administratives et juridiques de partage de l'action sécuritaire à l'intérieur de nos frontières. Fouettées par l'impact majeur des attentats de 2015 et 2016, de nombreuses avancées opérationnelles et institutionnelles peuvent être déjà relevées dans cette perspective. Et pourtant... Elles semblent encore timides ; leur efficacité se voit contestée⁽¹⁴⁾. L'heure est venue de changer d'échelle, d'élargir le spectre de veille, de comprendre et accepter l'*extension du domaine de la lutte*.

Nos avant-postes se déploieront encore *là-bas*, mais aussi *ici*, et pas seulement sur un plan strictement militaire.

Pourquoi ces avant-postes seraient-ils prêts à combattre, voire se sacrifier ?

« La force morale plus que le nombre des soldats décide de la victoire. »⁽¹⁵⁾

Réfléchir au déploiement stratégique de nos avant-postes dans un univers en mouvement accéléré, c'est aussi s'interroger sur ce que l'on défend. Le rêve européen

(14) « *Sentinelle*, dont l'efficacité globale a été contestée dans plusieurs rapports d'experts ou de parlementaires, a toutes les chances d'évoluer après la présidentielle, comme le souhaitent plusieurs candidats. Risques d'incidents, mauvaise complémentarité avec les forces de police, surchauffe des armées, fragilisation de leur valeur dissuasive, tels demeurent ses défauts majeurs. », Nathalie GUIBERT, *Le Monde*, 4 février 2017.

(15) Napoléon BONAPARTE, en 1809, cité par Lucian REGENBOGEN dans son recueil *Napoléon a dit – aphorismes, citations et opinions*, Les belles lettres, p. 28.

s'essouffle ; la France est divisée. La stratégie de fragmentation de l'ennemi est peut-être en œuvre. Si tel est le cas, sans doute convient-il alors d'abord de se demander pourquoi, plutôt que de céder à notre tour à l'anathème. Cet effort profond d'introspection s'avère hors de notre champ d'étude, mais il ne peut être tu poliment sinon lâchement. Il souligne à ce stade l'impératif des forces morales, éclairées par une parole lucide et armée ⁽¹⁶⁾, apte à dénier pied à pied, sans esprit de recul, la communication redoutablement séduisante et mortifère de l'EI ou la manipulation, numérique, asservissante et éhontée, de la réalité par les séides de Vladimir Poutine ⁽¹⁷⁾.

La cohésion de la Nation revêt une importance existentielle ; celle de ses avant-postes devient un facteur-clé de succès stratégique.

Nous allons y revenir au travers de la préparation des troupes, des états-majors et des chefs appelés à les armer. Nous préciserons aussi pourquoi nous parlons d'avant-postes de forces légères, au-delà du clin d'œil au colonel de Brack.

Vaincre à nouveau : *fighting spirit*, coup d'œil du chef et fluidité des états-majors

Des guerriers pour engager le combat : la primauté de la Force

Le durcissement et la complexité des opérations menées par nos armées depuis quinze ans nous rappellent que la guerre est un métier. Alors que celle-ci redevient plus perceptible dans l'esprit de nos concitoyens et plus présente dans leurs vies, consciemment ou non, il semble vital de remettre la Force, éclairée et maîtrisée, au cœur de notre société.

La Force, ce sont d'abord nos hommes de guerre, quel que soit le champ de leur action.

Doivent-ils être les mêmes *ici* et *là-bas* ?

Aujourd'hui, sans doute oui. D'abord parce que la Nation intègre à marche forcée l'impérieuse nécessité de se défendre jusque dans son sanctuaire. Ensuite parce que les armées sont confrontées au défi de leur attractivité – c'est tout le sens de la campagne de recrutement de l'Armée de terre.

Mais demain, dans dix ans, probablement non. Tout simplement parce que les hommes sont différents et les besoins de la Nation multiples. Les aspirations de notre jeunesse méritent d'être comblées selon un spectre beaucoup plus large, conciliant son sens de l'intérêt général et son souci de la vie personnelle. Certes, de nombreux jeunes hommes et femmes se sont présentés au recrutement en réaction aux attentats commis sur notre sol. Tous ne sont pas restés jusqu'au bout de leur formation initiale. La tentation serait grande alors de vilipender la versatilité de la génération *zapping*. Il s'avère mille fois préférable de contrebattre ce lieu commun, car la réalité est plus nuancée. Souvent, ceux qui partent s'orientent vers un métier de pompier, d'ambulancier,

(16) Cf. *Paroles armées*, Philippe-Joseph SALAZAR, 2015. Cet ouvrage mériterait d'être étudié dans toutes les écoles préparant les élites civiles et militaires de la Nation.

(17) Marc NEXON, « Gerasimov, le général russe qui mène la guerre de l'information », *Le Point.fr*, 2 mars 2017.

de policier, de vigile, d'acteur social. Le besoin de donner est là, en eux. Mais on peut donner ici, près des siens, dans son environnement immédiat, aux premiers avant-postes de la Nation. Notre État gagnerait sans doute à mieux intégrer ce besoin ⁽¹⁸⁾, car la réalité, c'est que tout le monde n'est pas fait pour une vie de soldat projeté au-delà de l'horizon lointain.

Héritiers de la culture expéditionnaire de nos armées, acceptant le risque comme un élément consubstantiel de leur engagement, les soldats de nos avant-postes sauront combiner rusticité et haute technologie.

Il ne s'agira pas simplement d'associer projection de quelques forces spéciales et mise en œuvre de drones et de missiles, bombes et obus dont il importe de relever au passage la précision toujours plus grande des effets. Il s'agira surtout de cultiver et développer encore les qualités foncières, techniques et morales de soldats, marins et aviateurs aptes à vivre et combattre dans des milieux hostiles, abrasifs, jusqu'*au cœur des ténèbres* s'il le faut.

Des hommes au sein d'unités capables de déployer un « camp romain » ⁽¹⁹⁾ au milieu du désert, prouvant par-là à leurs ennemis, leur détermination à ne jamais subir les éléments ni, *a fortiori*, les hommes, comme le démontraient systématiquement les légions romaines. Capables surtout, comme elles, de les démonter le lendemain et les redéployer ailleurs *vite, fort et loin* ⁽²⁰⁾. Des hommes dans de petites unités totalement intégrées, dans leur style de manœuvre et d'application des feux comme dans la compréhension de leur environnement physique et humain, au contact de la population et des éléments naturels, à leur aise dans la troisième dimension, maîtrisant leur force et l'employant *sans exaltation mais sans inhibition*. À juste escient.

Des hommes observant l'ennemi, vivant comme lui, comprenant son but, sublimant sa tactique. Dans la postface de son œuvre, le colonel de Brack écrivait ceci des cosaques qu'il combattit : « quelques officiers qui n'ont pas fait la guerre, ou qui l'ont faite autre part qu'aux avant-postes, ont pris la tâche de parler de ces cavaliers avec mépris ; ne les croyez pas. L'injustice envers son ennemi est toujours une mauvaise et fautive politique (...) Demandez l'opinion que conservent des cosaques, nos illustrations militaires (...) nos intrépides chefs (...) Il vous diront que des cavaliers légers, qui, comme les cosaques, entourent l'armée d'un réseau de vigilance et de défense impénétrables, qui harassent l'ennemi, qui donnent presque toujours des coups et n'en reçoivent que fort peu, remplissent complètement et parfaitement le but que doit se proposer toute cavalerie légère ». Voilà le *fighting spirit* des avant-postes.

Aptes à délivrer des feux rapides et précis, au contact et dans la profondeur, les soldats de nos avant-postes seront des guerriers naturellement mobiles, au mieux avec l'appui d'une

(18) « Armées, service civique ou autre, il y a actuellement déjà plus de volontaires que de places disponibles ! C'est donc d'abord à ceux-là qu'il faut répondre en inversant peut-être l'idée d'obligation : plutôt qu'un jeune effectuant son service obligatoire, que ce soit d'abord l'État qui soit obligé de répondre à un jeune voulant servir son pays en donnant six mois de sa vie à la Défense ou pour aider les personnes âgées, par exemple. », Jean-Dominique MERCHET, *La Dépêche.fr*, 6 janvier 2017.

(19) La plateforme opérationnelle désert de Gao, au Nord-Mali, fut conçue dans cet esprit au printemps 2013, par la force *Serval*.

(20) Devise de la 6^e Brigade légère blindée (6^e BLB), grande unité des forces terrestres de l'armée française.

capacité d'aéromobilité dédiée, au moins par leur souci constant d'investir la totalité du milieu dans lequel ils évolueront, quel qu'il soit, sans jamais perdre le fil de son tissu humain.

Ce tissu humain existe-t-il dans les autres dimensions que celles des villes et des campagnes ? Oui. La 3^e dimension n'est qu'une extension recouvrante des domaines terrestre et maritime. La mer comme milieu liquide s'infrastructure de plus en plus, depuis la réalité des plateformes pétrolières et des champs d'éoliennes jusqu'au projet « d'îles artificielles ancrées sur les fonds marins sous forme de plateformes modulables reliées les unes aux autres et utilisant l'énergie solaire »⁽²¹⁾, véritables villes du futur fondées en toute indépendance, en dehors de tout cadre étatique. Ces espaces en devenir seront investis d'une manière ou d'une autre ; les soldats de nos avant-postes y interviendront et sans doute pourrions-nous utilement repenser le développement des confettis de l'empire perdu, ces bouts de France conservés dans tous les océans. Pourquoi pas une base scientifique et militaire sur l'îlot de Clipperton, par exemple ? Aujourd'hui, le canal du Panama au large duquel il se situe ne constitue pas le point de passage le plus stratégique pour la France. Qu'en sera-t-il demain ? Le déploiement conjoint de militaires et de scientifiques, de jeunes hommes et femmes mus par l'appel du large et l'enthousiasme de l'aventure pionnière, servirait la dynamique d'installation aux marches stratégiques de notre pays, non pas de citadelles refermées sur elles-mêmes et figées dans l'illusion d'une nouvelle ligne Maginot, mais bien de points d'appui pour évoluer dans un espace sujet à l'infiltration de l'ennemi, préparer, précéder puis soutenir l'engagement de forces plus importantes. C'était du reste voici plus de trois siècles l'esprit des places fortes de Vauban, qui dessinèrent le contour de notre territoire tout en permettant une conception dynamique de la projection de puissance à partir de ces points d'appui. Il est temps d'accorder cette vision avec celle de notre monde pluridimensionnel. Ce n'est pas non plus de la science-fiction que d'imaginer des soldats dans l'Espace extra-atmosphérique, quand celui-ci se voit exploité de plus en plus intensément par les puissances émergentes⁽²²⁾. Dans dix ans, des militaires y seront peut-être nécessaires pour protéger nos systèmes de communication, d'observation et de renseignement autrement qu'en se reposant uniquement sur un bouclier d'essaims de satellites ou d'armes à énergie dirigée depuis la surface terrestre. L'homme y aura sa place. Dans le même temps, il lui faudra, à partir d'avant-postes numériques, reconquérir le cyberspace pollué, inondé par ses avatars et autres robots numériques interactifs.

Les hommes déployés sur nos avant-postes seront des combattants à l'esprit *joint*⁽²³⁾, intégré, parés pour les prémices d'une guerre totale, hybride ou conduite selon une dimension particulière.

Des chefs pleinement investis à leur tête : l'Honneur du commandement

« Le génie militaire est un don du ciel, mais la qualité essentielle d'un général en chef est la fermeté de caractère et la résolution de vaincre à tout prix. »⁽²⁴⁾

(21) « La première ville flottante sera-t-elle en France ? », *Le Point.fr*, 6 janvier 2017.

(22) « L'Inde met en orbite un record de 104 satellites en une seule mission », *Le Monde.fr*, 15 février 2017.

(23) *Joint* est le mot anglo-saxon signifiant interarmées, terme que l'on pourrait comprendre ici de façon plus large au sens interservices, interagences.

(24) Napoléon BONAPARTE, en 1820, cité par Lucian REGENBOGEN, op. cit., p. 28.

Pour commander les hommes, il faut des chefs. Pour les mener à la victoire, il faut les avoir formés dans cette perspective. C'est le sens de la devise de l'École spéciale militaire de Saint-Cyr – « ils s'instruisent pour vaincre » – et c'est la terrible leçon de l'histoire lorsque ce devoir est négligé, lorsque cette impérieuse nécessité n'irrigue plus de son sang vif le corps tout entier de la hiérarchie militaire. Avant de tomber en héros de la Résistance, en parfait accord entre ses écrits, ses paroles et ses actes, le professeur et capitaine Marc Bloch en témoigna durement dans *l'Étrange défaite*, par la peinture de chefs dépassés par les événements du terrible printemps 1940, sidérés par le désastre qui les clouait sur place tandis que les chars et l'aviation ennemie déferlaient sur le pays.

Les chefs sont investis dans leur commandement. Aux avant-postes, la formule rituelle et consacrée prend son sens entier ⁽²⁵⁾.

De fait, l'aptitude à commander au feu ne s'improvise pas ; elle se prépare. Parfois tout au long d'une vie d'officier, jusqu'à l'instant de vérité, celui précisément où l'on aura besoin d'un chef. Elle ne se prépare nulle part mieux qu'aux avant-postes, là où la confrontation peut surgir à tout moment, sous toutes les formes. Là où le coup d'œil est vite requis. Là où, très tôt, se forment le sens des responsabilités et, parfois, *l'étincelle de la grande ambition*. Là où naît la conscience profonde de l'humanité. « Mon poste aux frontières m'avait montré une face de la victoire qui ne figure pas sur la Colonne Trajane », écrit l'empereur Hadrien dans ses mémoires ⁽²⁶⁾, sous la plume de Marguerite Yourcenar, en se revoyant jeune officier aux légions de Rome.

Les avant-postes de forces légères restent la première école des chefs qui y éprouvent leur résistance physique et leur courage moral, tout en formant leur jugement.

Ils poursuivent ensuite leur trajectoire dans les armées ; leur gestionnaire y veille en alternant les affectations dans le corps de bataille et dans l'administration centrale, testant leur faculté d'adaptation, stimulant leur puissance de travail, élargissant leur champ de connaissances et de compétences tactiques et techniques. Car ils devront bientôt retourner à d'autres avant-postes, dont la constellation s'organisera selon l'articulation tactique, opérative et stratégique de notre chaîne de commandement. Nous reviendrons plus loin sur la subsidiarité induite, réelle et non partielle.

À chaque niveau, un chef. Clairement investi.

Apte à commander comme à être commandé, dans toutes les dimensions. Ce qui ne s'improvise pas non plus. D'autant moins que « l'affaiblissement, voire la disparition des frontières entre milieux, accélèrera d'autant le rythme de l'affrontement. Les armées devront, elles aussi, être à même de passer d'un milieu à l'autre avec le moins de ruptures possibles » ⁽²⁷⁾. Typiquement, les chefs devront être rompus à l'organisation du commandement prévalant dans le cadre complexe d'une opération amphibie, avec la bascule – ou non – du commandement de la mer vers la terre, dans

(25) « Vous lui obéirez en tout ce qu'il vous commandera pour le bien du service, le respect des règlements, l'observation des lois et le succès des armes de la France ».

(26) Marguerite YOURCENAR, *Mémoires d'Hadrien*, Édition Folio, 2014, p. 84.

(27) *Environnement opérationnel futur 2035*, production interarmées, octobre 2016.

le prolongement d'une phase de planification à la mer et de mécanisation conjointe, en fonction des circonstances et de l'atteinte des objectifs opérationnels.

La logique *supported/supporting* – menant/concourant s'imposera partout.

Dans cette perspective, il semble particulièrement pertinent de poursuivre annuellement les campagnes d'application des officiers-élèves de la Marine nationale sous leur format actuel, sans jamais en dégrader l'ambition opérationnelle au sens de l'instruction des futurs chefs, de l'entraînement interarmées et du prépositionnement opérationnel. Formant le groupe « Jeanne d'Arc », le bâtiment de projection et de commandement (BPC) *Mistral* et la frégate Courbet ont ainsi appareillé de Toulon ⁽²⁸⁾ avec à bord du BPC, outre l'équipage et les jeunes officiers sortis de l'École navale ou d'autres organismes (commissaires-élèves, administrateurs des affaires maritimes et médecins des armées), des aéronaves du 3^e Régiment d'hélicoptères de combat (3^e RHC) et un Groupement tactique embarqué (GTE) armé par des éléments du 21^e Régiment d'infanterie de Marine (21^e RIMa), du 3^e Régiment d'artillerie de marine (3^e RAMa), du 1^{er} Régiment étranger de génie (1^{er} REG) et des véhicules blindés légers du Régiment d'infanterie-chars de Marine (RICM). Des détachements de l'*US Marine Corps* et de la *Royal Navy* britannique complètent ce dispositif en apportant une dimension interalliée à un pion de prépositionnement stratégique, véritable avant-poste mobile, polyvalent et cohérent, croisant de la Méditerranée jusqu'en mer de Chine en passant par le canal de Suez et le détroit du Bab-el-Mandeb.

Mais laissons marins et marsouins voguer vers leur destin et penchons-nous maintenant sur ceux sur lesquels les chefs peuvent compter dans leur solitude : leurs états-majors.

**Des états-majors comprenant l'intégralité de l'action :
l'impératif du Discernement**

Nous avons parlé de *compréhension* ⁽²⁹⁾ dans les lignes qui précédaient, au sens de l'intelligence, c'est-à-dire de la capacité à discerner, saisir la complexité des liens et les démêler si nécessaire. De fait, l'ouvrage prospectif des armées – *Environnement opérationnel futur 2035* – s'ouvre sur ces propos : « en assurant une bonne compréhension des milieux et des perceptions humaines ainsi que l'adéquation entre le sens et la cohérence de nos actions et anticipations, nous offrirons des conditions pérennes de confiance et de détermination, au service de la stratégie et de la résilience de la Nation ». Or, si le chef s'impose par son coup d'œil, son intuition doit se renforcer, se confirmer ou évoluer grâce à l'intelligence collective de son état-major. Il faut avoir servi au sein d'un État-major de force prépositionnée (EMIA) ou dans un Poste de commandement interarmées de théâtre (PCIAT) pour percevoir à quel point cet entourage du chef lui est précieux à la pointe de l'action extérieure de notre pays.

(28) Jean-Louis VENNE, « Le groupe Jeanne d'Arc a quitté Toulon », *Mer et Marine*, 1^{er} mars 2017.

(29) C'est le premier des huit facteurs de supériorité opérationnelle définis par l'Armée de terre dans son document prospectif, *Action terrestre future*, septembre 2016.

Aux avant-postes, les états-majors s'articulent autour d'un noyau dur concentré sur la mise en œuvre des fonctions opérationnelles de contact et l'intégration des appuis, agrégeant autant que de besoin les fonctions d'environnement.

La force d'un état-major ne tient pas tant dans son nombre d'officiers traitants que dans l'organisation de son travail éclairée par des éléments d'appréciation globale et ciblée. Le cœur de la fonction de combat est pensé par des guerriers ; l'amplitude des effets est suggérée par la combinaison des points de vue d'autres spécialistes. Le chef de guerre compte déjà souvent près de lui un conseiller politique, un juriste, un communicant. Des équipes agissant sur la perception de l'environnement opérationnel (APEO) existent aussi aux niveaux tactiques, opératifs et stratégique, dépassant le cadre trop restrictif des seules affaires civilo-militaires pour investir plus largement celui de l'influence. Ce champ de l'influence constitue l'un des domaines d'excellence de nos forces spéciales dont la capacité de liaison-contact s'avère infiniment précieuse aux avant-postes, en amont de l'action, pendant et encore après. La force crée les conditions du dialogue lorsqu'elle est crédible. Le dialogue est favorisé par le travail d'influence. Les options qui s'en dégagent sont mises en œuvre sous couvert de la force. Pour parvenir à cette synthèse qui préserve autant que possible la vie humaine, limitant l'emploi des armes au strict nécessaire pour garder l'ascendant et imposer une volonté éclairée, il faut des états-majors au plus près de l'action. Peut-être le développement de l'intelligence artificielle permettra-t-il d'élaborer des algorithmes proposant ses options au décideur, en intégrant toujours mieux les multiples données de crises complexes. Il manquera encore le ressenti de l'homme, l'expérience grandie dans la chair et sans doute aussi, une part d'irrationnel, la compréhension d'autres cultures. En outre des conseillers cités plus haut, l'intégration de jeunes chercheurs, de thésards en sciences économiques, sociales et politiques, agronomie ⁽³⁰⁾, ethnologie, histoire des civilisations et théologie pourraient être favorisée au sein des états-majors déployés aux avant-postes, en recourant à la réserve opérationnelle ou en développant l'idée d'un service national non universel mais offert à ceux qui y aspirent dans leur domaine de compétence.

Aux avant-postes, les états-majors seront d'abord taillés pour comprendre, discerner.

Ce qui est vrai aux avant-postes extérieurs l'est aussi à l'intérieur. La perception des signaux faibles s'avère plus que jamais vitale, au regard de la menace pesant sur le pays. Relevant que le déroulement des attentats commis sur notre sol ces deux dernières années se conformaient « à la doctrine et au mode d'emploi que l'on trouve dans *L'appel à la résistance islamique mondiale* de l'ingénieur syrien Abu Musab al-Suri aussi bien que dans le *Management de la sauvagerie* d'un auteur non identifié, qui signe Naji », Gilles Kepel déplore ainsi dans son dernier ouvrage l'ignorance des avertissements qui nous ont été adressés, « au mépris du savoir déconsidéré des arabisants, de la sociologie dépréciée des enquêtes de terrain dans les quartiers populaires et de la psychologie dénigrée qui a également mis au jour les symptômes cliniques de ces phénomènes dans les centres de santé depuis une décennie » ⁽³¹⁾. Faudra-t-il attendre une décennie pour prendre en compte *a posteriori* ce que nous savons aujourd'hui du

(30) Gaëlle LALEIX, « Élevage : un master en pastoralisme pour les pays sahéliens », *RFI.fr*, 9 mars 2017.

(31) Gilles KEPÉL, *La fracture*, Gallimard, 2016.

radicalisme dans les prisons ? Nos services de renseignement et nos forces de police ont certes opéré une première révolution culturelle dans leur façon d'aborder la sécurité intérieure, mais beaucoup reste à faire. Tout en conservant sa culture expéditionnaire (les avant-postes extérieurs), l'Armée de terre peut voir dans sa reterritorialisation (les avant-postes intérieurs) un enjeu majeur pour la Nation. Ses états-majors tactiques de régiment et ses postes de commandement de brigade constituent autant d'outils de commandement en mesure de prendre en compte, localement, temporairement, une situation totalement dégradée. En intégrant des cellules de liaison de tous horizons.

Aux avant-postes, les états-majors seront interagences par construction et nécessité.

« Force et Honneur », déclaraient sobrement les tribuns des légions en ligne de bataille face aux barbares, aux premières minutes épiques de *Gladiator* ⁽³²⁾. « Force et Honneur + Discernement », pourrions-nous ajouter pour proposer une devise des avant-postes destinés à encaisser le premier choc. Mais ils ne seront pas seuls. L'heure est venue d'imaginer comment les armées pourraient toujours les déployer en les distinguant de notre corps de bataille et de notre force de dissuasion.

Vaincre inlassablement : initiative, réserve stratégique et vigilance

Le courage de la confiance

Revenons tout d'abord au principe de subsidiarité. Si un chef est investi dans son commandement, il l'est totalement. Aux avant-postes, il détient le contrôle opérationnel – l'*OPCON* – des moyens placés sous son autorité. Il est naturellement connecté au niveau stratégique, celui qui assure le commandement opérationnel – l'*OPCOM* – de toutes les forces prépositionnées ou déployées, compte tenu de l'impérieuse contrainte d'immédiateté de la connaissance rendue possible par les nouvelles technologies de l'information et de la communication. Mais à l'avenir, il devra aussi être capable de s'en affranchir. « Ne s'appuyer que sur des systèmes numériques représente en effet un risque de dépendance aux outils digitaux comme à la couverture satellitaire. Il s'agit donc de réfléchir aux solutions qui seront, pour ce faire, les plus appropriées (redondance, robustesse, moyens dégradés) » ⁽³³⁾. Le maintien de compétences rustiques et entretenues en matière de télécommunication, de navigation, mais aussi et surtout d'initiative s'impose. Traduction pour le chef : aptitude à décider en connaissance de cause, quoiqu'il arrive. Ce qui suppose, outre la préparation à cette responsabilité assumée pour la Nation, évoquée plus haut, la confiance de l'échelon supérieur, militaire et politique, c'est-à-dire la solidarité de la chaîne de commandement.

L'esprit d'initiative indispensable aux avant-postes ne peut être un vain mot ; ce sera toujours une condition du succès.

Déjà, les commandants de forces en opération (*COMANFOR*) et les commandants de forces prépositionnées à l'étranger (*COMFOR*) ou de souveraineté sur nos territoires d'outre-mer (*COMSUP*) exercent des responsabilités élevées, en liaison avec

(32) Film américano-britannique de Ridley SCOTT, produit par DreamWorks Pictures et Universal Pictures, 2000.

(33) *Environnement opérationnel futur 2035*, op. cit.

l'autorité civile (ambassadeur, haut représentant ou préfet). Durer sur un poste se montre nécessaire pour y être identifié suffisamment sûrement par l'ensemble des acteurs, comprendre l'environnement, influencer, décider. La durée de déploiement des *COMANFOR* tend à s'allonger. Elle est aujourd'hui d'un an pour l'officier général placé à la tête de l'opération *Barkhane*. Peut-être devrait-elle encore être augmentée, à l'image des *COMFOR* et *COMSUP* affectés à leur poste pour deux ans. *L'illusion des options courtes* a vécu ; les crises se résolvent dans le temps long et dans la profondeur d'un pays, de son peuple, de son environnement régional. Les avant-postes de forces légères ont vocation à être renforcés quand le besoin se fait sentir ; ils demeurent quand l'engagement du renfort n'est plus nécessaire. Ils gardent la mémoire en leurs chefs et par les états-majors qui les servent.

L'esprit d'initiative se conforte dans la durée ; les avant-postes seront commandés par des hommes parés pour les longues campagnes.

Mais si les chefs et leurs états-majors sont appelés à de plus longs déploiements qu'aujourd'hui, qu'advient-il de leurs troupes ?

Des ressources véritablement différenciées

Aujourd'hui, un *COMANFOR* peut voir défiler plusieurs groupements de forces dans le temps de sa mission. Cette rotation implique de nombreuses opérations de projection, de relève, de prise de consignes et de transmission de contacts de chefs à chefs, au niveau des groupements et sous-groupements, avant le transfert d'autorité. On trouve là une part de la force de nos armées, dans leur aptitude à s'appropriier leur environnement. On y trouve aussi une part significative de la motivation de nos soldats, leur désir sain d'engagement et d'aventure. Mais comme nous l'avons suggéré plus haut, tous nos jeunes ne sont pas faits pour le service lointain tandis que les effectifs ne s'avèrent pas extensibles à l'infini. Avec le déploiement de milliers de soldats sur le territoire national dans le cadre de l'opération *Sentinelle*, le cycle de vie des forces terrestres a vu non seulement leur préparation opérationnelle générique se dégrader pour garantir le rythme de projection en opérations intérieure et extérieure, mais aussi l'échelon national d'urgence (ENU) – successeur du dispositif d'alerte *Guépard* – perdre sa réalité, hors composante parachutiste. Question de priorité parfaitement comprise sur le moment, mais qu'il importe de réviser pour retrouver du souffle, de la profondeur et des marges de manœuvre. Retrouver une capacité de réaction, reconstituer la réserve stratégique. Il n'est pas absurde de penser que le cœur de nos avant-postes pourrait être armé d'ici dix ans par davantage de personnel en campagne longue. C'est déjà la tendance que l'on observe sur nos points d'appui outre-mer et à l'étranger, avec un allongement de la durée d'affectation du personnel permanent. Durer à l'extérieur, loin de son pays, dans des conditions parfois éprouvantes. Durer aussi à la mer, ou sous la mer. Naviguer, survoler, crapahuter. Comprendre le milieu dans son corps et dans sa tête. Parcourir le désert à la manière des compagnies méharistes, tout en intégrant la combinaison gagnante du *pick-up* et du téléphone satellitaire ; combattre la guérilla tout en faisant siennes ses techniques, à la façon d'un Lawrence d'Arabie. « Sahéliser *Barkhane* », selon la formule de l'actuel *COMANFOR*. Amariner les troupes de débarquement, forger les montagnards et les forestiers sur les cimes et dans la jungle.

Se préparer enfin à durer bientôt dans l'Espace, à la manière de l'équipage de la Station spatiale internationale (*ISS*).

Le service aux avant-postes requiert des troupes dans la durée. Bien y veiller, c'est aussi préserver la réserve stratégique.

Cela ne signifie pas « une armée à deux vitesses ». Il est temps de clore le chapitre de la professionnalisation de l'Armée de terre, ouvert lorsque les unités du corps blindé mécanisé ne partageaient pas l'expérience opérationnelle de celles de la Force d'action rapide. L'Armée de terre tout entière s'est aguerrie successivement dans les Balkans, en Afghanistan et en Afrique. Aujourd'hui, elle doit tenir les avant-postes, sécuriser notre territoire et se préparer inlassablement à une guerre plus dure, perspective somme toute beaucoup moins improbable qu'il y a vingt ans, lorsque le service militaire fut suspendu. Il en est de même pour la Marine nationale, dont les bâtiments à la mer sont autant d'avant-postes en mouvement, sur nos approches maritimes et de par le monde, et pour l'Armée de l'air, dont les bases aériennes projetées en Jordanie ou au Niger s'avèrent indispensables non seulement à la mise en œuvre de nos capacités aéroportées de renseignement et de frappe, mais aussi aux bascules d'effort sur le plan opératif par l'aérotransport. Dans le même temps, notre Marine et notre aviation doivent impérativement se préparer à faire face à un ennemi qui disposera, lui, de capacités similaires en mer et dans les airs. Enfin, elles portent chacune une part de la responsabilité de notre dissuasion nucléaire.

Les avant-postes sont par essence constitués de forces légères, soutenues par le corps de bataille principal de nos trois armées qui doit se préparer au pire tout en garantissant la crédibilité de notre force de frappe et en se tenant prêt à porter secours aux avant-postes.

Le dispositif de défense de notre pays s'articule donc simplement en conciliant préservation du sanctuaire et influence extérieure, avec une ouverture très vive au monde.

Des forces sur le qui-vive

Ce sont les avant-postes qui tiennent ce dispositif de défense en éveil.

Ce sont eux qui veillent sur les signaux faibles tout en diffusant leur propre influence et en générant le sentiment de sécurité attaché à leur force vigilante.

C'est vrai à l'extérieur, où le déploiement d'un élément des forces françaises est immédiatement perçu par les populations comme un signe fort, une promesse de protection et de stabilisation. L'assurance que les colonnes françaises, ses avions, ses canonnières sont derrière, avec leur force mais aussi les lumières de notre pays, celles qui lui sont reconnues par-delà les tentatives d'intoxication ou les fautes de certains de ses enfants. Ainsi en fut-il des avant-postes de *Sangaris* dans la profondeur du territoire centrafricain jusqu'à leur transmission progressive aux Casques bleus, au fur et à mesure de la montée en puissance de la mission des Nations unies (*MINUSCA*), appuyée, rassurée, réassurée⁽³⁴⁾, confortée jusqu'au bout par les soldats français.

(34) La réassurance est aussi au cœur du concept de l'Otan *Enhanced Forward Presence* (EFP), en Europe de l'Est.

Ce pourrait être tout aussi vrai à l'intérieur de notre pays, dans nos campagnes où la population perd l'habitude de voir évoluer librement nos unités depuis que celles-ci concentrent leur entraînement dans des camps avant d'être projetées à l'extérieur ou déployées dans nos grandes villes aux côtés des forces de sécurité intérieure. Il y a matière à faire d'une pierre trois coups. D'abord, exploiter nos déserts militaires pour y redéployer nos grandes unités des forces terrestres, en autonomie totale. Simultanément, renouer les contacts avec tous les maillages de notre administration territoriale, les brigades de gendarmerie et les polices municipales, les élus et la population, comme lorsque l'on nomadise en brousse. Ensuite, s'y entraîner aux fondamentaux du combat en zone périurbaine, montagnaise ou semi-désertique – par exemple, dans les Grands Causses – tout en cultivant les interactions interarmées – pour la maîtrise de la troisième dimension, notamment – c'est-à-dire se préparer à une projection sur un théâtre d'opération exigeant. Dans le même temps, constituer de petites forces complètes, autonomes sur le plan logistique et cohérentes avec leur système de commandement, rappelables sur faible préavis pour prêter concours à l'autorité publique en cas de catastrophe ou d'intempéries. S'inscrire ainsi résolument dans une logique partenariale dont nous saurons cueillir les fruits. Enfin, *paré guerre*, contribuer par cette présence dissuasive au renforcement général du niveau de sécurité, *en mesure de* répondre instantanément à la demande de l'autorité politique en cas d'aggravation soudaine de la situation. Telle pourrait être la contribution des armées aux avant-postes intérieurs, ceux-ci ne pouvant pas leur être confiés *ab initio*, contrairement aux avant-postes extérieurs qu'elles sont les seules à même de diriger, en agrégeant des compétences aussi variées que nécessaire.

Vigilance tous azimuts, c'est la clé des avant-postes, à l'extérieur comme à l'intérieur.

Coopération, agilité, performance du commandement. Voilà trois facteurs de supériorité opérationnelle définis par l'Armée de terre pour inspirer l'action aux avant-postes, en outre de la *compréhension*, l'*endurance*, la *force morale* et l'*influence*, déjà évoquées. Seule la *masse* est absente de ce panorama. Mais en apparence, seulement. Car c'est elle qui, en France, à partir du corps de bataille principal, permet de « générer et entretenir les volumes de forces suffisants pour produire des effets de décision stratégique dans la durée »⁽³⁵⁾, ce qui constitue, sur les lignes de rupture stratégique, l'une des raisons d'être des avant-postes de forces légères.

Conclusion

Plongeons-nous quelques instants dans la science-fiction si féconde pour l'imagination galopante et laissons-nous porter dans l'univers de *Star Wars*, plus précisément dans son dernier épisode, *Rogue One*. Publié sur le site *Politico*, un court article tirait des parallèles entre ce film et la guerre au Moyen-Orient, la lutte contre le terrorisme islamiste. Comme le relève Vincent Lowy⁽³⁶⁾, la troupe de rebelles qui y affronte l'Empire est composée de mercenaires représentant des minorités, exécutant une

(35) *Action terrestre future*, septembre 2016.

(36) Vincent LOWY, « Géopolitique de *Rogue One* (ou comment dire au revoir à l'Amérique) », *The Conversation*, 20 janvier 2017, cité le même jour par Michel GOYA sur son compte Twitter.

mission délicate se terminant en apothéose avec la mort de ces combattants mal équipés et peu coordonnés mais héroïsés, harcelant avec succès les avant-postes d'un ennemi puissant et implacable s'employant à maintenir l'ordre dans la galaxie... L'analogie Empire/États-Unis – rebelles/terroristes est d'autant plus troublante lorsque l'on songe à notre propre position dans ce combat. Veillons à ce que le romantisme ne change pas de camp, entraînant avec lui notre référentiel de valeurs et diluant la légitimité de nos intérêts, chronique d'une défaite annoncée.

Pourquoi terminer sur une métaphore cinématographique ? Parce que l'audience du 7^e art est large ; parce que la guerre sera longue. Quel rapport avec les avant-postes ? La menace peut surgir de partout ; la constellation de nos avant-postes nous protégera de son « rideau vigilant et courageux ». Pourquoi des forces légères ? Parce qu'elles sont les plus à même de demeurer sur le qui-vive. Parce qu'elles forgent les chefs et parlent à la jeunesse. Parce qu'on y apprend la force, l'honneur et le discernement.

Éléments de bibliographie

Qu'il s'agisse d'essais, de beaux livres ou de romans, les ouvrages qui suivent ont inspiré la rédaction de ce document, soit du fait d'une étude récente et ciblée pour son élaboration, soit en raison d'une lecture plus ancienne et mûrie au fil de mes années de service.

Ouvrages de littérature générale et spécialisée

BENOÎT Christian, CHAMPEAUX Antoine, DEROO Éric et RIVES Maurice, *Des troupes coloniales aux troupes de Marine. Un rêve d'aventure 1900 – 2000*, Lavauzelle, 2000, 156 pages.

BLOCH Marc, *L'étrange défaite* (préface de Stanley Hoffmann), Édition Folio, 2015, 336 pages.

BRACK (DE) Antoine-Fortuné, *Avant-postes de cavalerie légère*, Carrefour du Net Éditions, 2011, 325 pages.

BUZZATI Dino, *Le désert des Tartares*, Édition du Livre de Poche, 2004, 288 pages.

CARRÈRE D'ENCAUSSE Hélène, *Catherine II. Un âge d'or pour la Russie*, Fayard, 2002, 656 pages.

CLAUSEWITZ (VON) Carl, *De la guerre*, Les Éditions de Minuit, 1955, 760 pages.

CONRAD Joseph, *Au cœur des ténèbres / Heart of darkness*, Folio bilingue, 1996, 336 pages.

FORCES FRANÇAISES DU CAP-VERT, *L'armée française au Sénégal, Deux siècles d'Histoire*, Presses de l'imprimerie La Rochette – Dakar, 2009, 101 pages.

HOUELLEBECQ Michel, *Soumission*, Flammarion, 2015, 300 pages.

HUBIN Guy, *Perspectives tactiques* (préface d'Hervé Coutau-Bégarie), Economica, 2003, 142 pages.

INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE (IHEDN), *EspritS de défense*, octobre 2016, 174 pages (www.ihedn.fr/sites/default/files/atoms/files/ihedn_esprits_de_dc3a9fense_2015_0.pdf).

JOURDIER François, *Indochine 1952 – 1954, Les Luc Binh, Souvenirs d'un marin du fleuve*, L'esprit du livre, 2009, 120 pages.

KEPEL Gilles, *La fracture*, Gallimard, 2016, 288 pages.

KHADRA Yasmina, *La dernière nuit du Raïs*, Pocket, 2016, 192 pages.

LARTÉGUY Jean, *Les centurions*, Presses de la Cité, 1960, 416 pages.

LAWRENCE Thomas E., *Guérilla dans le désert 1916 – 1918*, Éditions Complexe, 1992, 90 pages.

LE DRIAN Jean-Yves, *Qui est l'ennemi ?*, Éditions du Cerf, 2016, 80 pages.

Le Monde, L'atlas des empires, hors-série n° 18, octobre 2016, 186 pages.

LIAUTEY Hubert, *Paroles d'action, Madagascar – Sud-oranais – Oran – Maroc (1900 – 1926)*, Librairie Armand Colin, 1927, 480 pages (<http://gallica.bnf.fr/ark:/12148/bpt6k54616304>).

MALIS Christian, *Guerre et stratégie au XXI^e siècle*, Fayard, 2014, 352 pages.

PORTE Rémy, *Joffre*, Perrin, 2014, 432 pages.

PRATT Hugo, *Les scorpions du désert* (BD en 6 tomes) Casterman, 1977, 94 pages.

SALAZAR Philippe-Joseph, *Paroles armées, Comprendre et combattre la propagande terroriste*, Lemieux Éditeur, 2015, 264 pages.

SCHOENDOERFFER Pierre, *La 31^e section*, Fixot/La Table Ronde, 1992, 252 pages.

STRACHAN Hew, *The Direction of War, Contemporary Strategy in Historical Perspective*, Cambridge University Press, 2013, 335 pages.

TOLSTOÏ Léon, *La Guerre et la Paix* (2 tomes), Édition du Livre de Poche, 2010, 992 et 960 pages.

TULARD Jean, *Napoléon chef de guerre*, Éditions Tallandier, 2015, 384 pages.

YOURCENAR Marguerite, *Mémoires d'Hadrien*, Édition Folio, 2014 (1977), 384 pages.

Ouvrages prospectifs des armées

France

ÉTAT-MAJOR DES ARMÉES, *Cap 2020 – Transformons nos armées*, 2016.

ÉTAT-MAJOR DE L'ARMÉE DE TERRE, *Action terrestre future*, septembre 2016.

CENTRE D'ÉTUDES STRATÉGIQUES DE LA MARINE (CESM), *Ambition navale au XXI^e siècle*, octobre 2016.

ÉTAT-MAJOR DE L'ARMÉE DE L'AIR, *Unis pour faire face – Acte II*, 2016.

CENTRE INTERARMÉES DE CONCEPTS, DE DOCTRINES ET D'EXPÉRIMENTATIONS (CICDE), *Environnement opérationnel futur 2035*, octobre 2016.

Chine

OFFICE D'INFORMATION DU CONSEIL DES AFFAIRES D'ÉTAT DE LA RÉPUBLIQUE POPULAIRE DE CHINE, *Livre blanc : stratégie militaire de la Chine*, édition en langues étrangères, mai 2015.

Études collectives (dans l'ordre chronologique)

IHEDN - COMITÉ 2, *Comment concilier contre-espionnage et lutte antiterroriste ?*, novembre 2016.

ÉCOLES MILITAIRES DE DRAGUIGNAN (EMD), *3 ennemis et 2 manœuvres !*, novembre 2016.

CHEM - COMITÉ D, *Leçons à tirer des conflits récents*, décembre 2016.

IHEDN - COMITÉ 2, *Irak, Libye, Syrie : quels objectifs de guerre et quelles conditions du succès ?* (travaux en cours).

Articles en ligne, non cités en notes de bas de page (dans l'ordre chronologique)

SCHOGOL Jeff, « Marines want new technologies to take enemy beaches », *Marine Corps Times*, 22 octobre 2016 (www.marinecorpstimes.com/articles/marines-want-new-technologies-to-take-enemy-beaches).

MEYNIAL Claire, « Lori-Anne Thérout-Benoni : pour les « djihadistes » maliens, le fait religieux n'occupe pas une dimension centrale », *Le Point Afrique*, 8 décembre 2016, cité par Philippe Vial, référent académique du CHEM (<http://afrique.lepoint.fr/>).

PONCET Gueric, « Comment Pékin transforme des récifs en bases militaires », *Le Point*, 15 décembre 2016 (www.lepoint.fr/monde/comment-pekin-transforme-des-recifs-en-bases-militaires-15-12-2016-2090695_24.php).

PONCET Gueric, « Cyberguerre. Les câbles sous-marins, le maillon faible », *Le Point.fr*, 28 janvier 2017 (modifié le 15 mai 2017) – article citée notamment pour la carte.

« Ça se passe en Europe : aux Pays-Bas, d'anciens soldats de la guerre froide rappelés pour enseigner aux jeunes », *Les Échos*, 17 février 2017 (www.lesechos.fr/).

GALLOIS Dominique, « La course au réarmement s'amplifie dans le monde », *Le Monde Économie*, 20 février 2017.

Filmographie

À l'instar des romans cités plus haut, les films suivants ont contribué à construire ma vision du déploiement aux avant-postes.

WISE Robert, *La canonnière du Yang-Tsé*, film américain produit par 20th Century Fox, 1966.

SCHOENDOERFFER Pierre, *Dien-Bien-Phu*, film franco-vietnamien produit par TF1 Vidéo et Studiocanal, 1992.

EASTWOOD Clint, *Lettres d'Iwo-jima*, film américain produit par Warner Bros, DreamWorks SKG, Malpaso Productions et Amblin Entertainment, 2006.

MCKENNA Bruce, *The Pacific*, série télévisée américano-australienne, 2010.

GORDON Howard, *Homeland*, série télévisée américaine, 2011 – 2017.

Entretiens – Relectures

Compte tenu de l'exceptionnelle richesse des conférences données au CHEM et à l'IHEDN sur de multiples sujets militaires, stratégiques et généraux touchant de près ou de loin au thème de cette étude, mon parti pris a résolument consisté à mûrir la réflexion initiée par ces interventions. Dans le même temps, cette réflexion s'est structurée grâce à l'apport de plusieurs entretiens accordés dans le cadre de travaux collectifs de mes comités du CHEM et de l'IHEDN :

- Amiral Bernard ROGEL, Chef d'état-major particulier du président de la République, ancien Chef d'état-major de la Marine, ancien sous-chef opérations de l'État-major des armées (EMA) :
 - entretien le 2 novembre 2016, sur le thème « leçons à tirer des conflits récents ».
- Général d'armée Didier CASTRES, inspecteur général des armées (Terre), ancien sous-chef opérations de l'EMA :
 - entretien le 3 novembre 2016, sur le thème « leçons à tirer des conflits récents » ;
 - entretien le 26 janvier 2017, sur le thème « Irak, Libye, Syrie : quels objectifs de guerre et quelles conditions du succès ? ».
- Amiral Philippe COINDREAU, major général des armées, ancien commandant de l'opération *Harmattan* (mars à septembre 2011) :
 - entretien le 3 mars 2017, sur le thème « Irak, Libye, Syrie : quels objectifs de guerre et quelles conditions du succès ? ».
- Général de brigade Pierre Gillet, commandant les Écoles militaires de Draguignan, ancien commandant de *Sangaris* (mars à septembre 2015), ancien chef du bureau planification (J5) du Centre de planification et de conduite des opérations (CPCO) de l'EMA :
 - entretien le 10 octobre 2016, sur le thème « leçons à tirer des conflits récents » ;
 - nombreux échanges sur le thème « avant-postes de forces légères ».

Enfin, ce document a fait l'objet de relectures et réflexions croisées avec :

- Vice-amiral François CLUZEL, ancien amiral adjoint opérations de l'amiral commandant la force d'action navale, ancien commandant de l'opération *Heracles* (décembre 2001 à juillet 2002) ;
- Général de division Laurent KOLODZIEJ, officier général relations internationales de l'État-major de l'Armée de terre (EMAT), ancien commandant de la brigade interarmes *Serval* (mai à septembre 2013) ;
- Ingénieur en chef de l'armement Olivier BEAURENAUT, auditeur au CHEM ;
- Plusieurs membres de l'équipe de commandement du général de brigade Pierre GILLET lorsqu'il commandait la force *Sangaris* (mars à septembre 2015) : son assistant militaire, le chef de bataillon Pierre-Antoine SIMON, et ses deux conseillers politiques successifs, Edouard GENDROT et Simon BROCAS ;
- Véronique SIMON, chargée des relations avec la presse et des relations publiques pour la Fondation Arc pour la recherche sur le cancer, que je remercie pour son regard extérieur et attentif.

Commander les opérations en 2030 : quel équilibre entre centralisation réactive et réalités de terrain ?

Thierry GARRETA

| Colonel (air), auditeur de la 66^e session du CHEM.

L'Armée de l'air française a fait le choix en 2013 de regrouper le commandement de l'ensemble des opérations aériennes nationales, au-dessus de la France ou sur les théâtres extérieurs, au sein d'un seul centre de commandement (le CNOA) sur la Base aérienne de Lyon–Mont-Verdun. Cette décision, en rupture avec la pratique habituelle qui consiste à déployer les centres de commandement – les *C2* ⁽¹⁾ en vocabulaire militaire – au plus près des conflits, fut motivée par la volonté d'optimiser l'emploi des moyens aériens, de gagner en réactivité, de diminuer les ressources humaines engagées dans la planification et la conduite des opérations. Mais cette centralisation du commandement fut également permise par l'émergence de nouvelles capacités techniques, comme les liaisons de données tactiques, permettant au centre de Lyon de suivre en direct les positions des avions où qu'ils soient en zone d'opérations, ou comme l'avion de transport stratégique *A400M Atlas*, dont le rayon d'action et la capacité d'emport lui permettent de desservir plusieurs théâtres au cours d'une même mission, en rupture avec ses prédécesseurs comme le *C-160 Transall*.

Ce nouveau modèle, décalé du modèle terrestre et non conforme à la doctrine de référence, est-il innovant et en avance sur son temps, en phase avec les études prospectives de l'Otan dans ce domaine, ou simplement une réponse provisoire à un manque de ressources humaines en mesure d'armer les *C2 Air* ? Les progrès technologiques, comme les drones, les véhicules autonomes et la numérisation du champ de bataille, conduiront-ils à développer cette pratique en centralisant à l'extrême le commandement des opérations à Paris, répondant ainsi aux exigences toujours plus fortes de réactivité et de détail de la part du niveau politique, sollicité en permanence par des médias hyperconnectés, une justice pressante et une opinion publique exigeante ?

Après un rappel des évolutions récentes suivi d'une revue des opportunités offertes par l'innovation technologique des outils de commandement et de conduite des opérations, des nouvelles capacités techniques civiles et militaires, une analyse des exigences du commandement en opérations et des réalités de terrain – relations

(1) *C2* : *Command and Control*. Abréviation usuelle du centre de commandement, généralisée au sein des forces alliées occidentales.

humaines, connaissance des acteurs locaux, commandement des hommes, résilience – permettra d'évaluer l'équilibre à préserver dans dix ans, entre une centralisation devenue possible et une vision plus traditionnelle des structures de commandement, en dégageant quelques tendances d'organisation du C2 du futur.

Le commandement des opérations en mutation

Aujourd'hui en France, comme dans la plupart des pays membres de l'Otan, la structure de commandement des engagements opérationnels suit les directives des doctrines de référence ⁽²⁾. Quatre niveaux décisionnels y sont définis :

1. **Le niveau politique** : le président de la République et chef des armées fixe la stratégie de l'État, englobant les domaines militaire, sécuritaire, diplomatique, économique et culturel.

2. **Le niveau dit stratégique** : le Chef d'état-major des armées (Céma), en tant que conseiller militaire du Gouvernement et commandant opérationnel des forces, traduit les objectifs politiques en objectifs militaires et en commande leur réalisation.

3. **Le niveau dit opératif** : le chef de l'opération, placé sur le théâtre d'opérations, sous les ordres du Céma resté à Paris, intègre les forces de chaque armée et fait exécuter les actions concrètes qui découlent des objectifs stratégiques.

4. **Le niveau dit tactique** : le chef de composante (terre, air, mer, forces spéciales), déployé au plus près des actions, sous les ordres du chef de l'opération, conduit les opérations sur le terrain au quotidien.

Depuis quelques années, on constate certaines adaptations de cette structure, vers davantage de centralisation, qui conduisent à penser que la pratique puis la doctrine pourraient évoluer dans les années à venir. Comme évoqué en introduction, l'Armée de l'air a rompu avec le schéma traditionnel en rapatriant en 2013 le niveau opératif de l'opération *Barkhane*, opération en cours de lutte contre le terrorisme dans la Bande sahélo-saharienne ou BSS (Mauritanie, Mali, Niger, Burkina-Faso, Tchad) du PC de N'Djamena au Tchad, à Lyon en France. Le terme de « C2 Full Rear » est employé pour qualifier cette organisation du C2 « Air ».

De plus, la structure elle-même de l'opération *Barkhane* est innovante, rassemblant plusieurs anciennes opérations locales (*Épervier* ⁽³⁾, *Serval* ⁽⁴⁾...) sous un seul commandement régional, centralisé à N'Djamena, commandant à des forces interarmées déployées dans cinq pays. Le Centre de planification et de conduite des opérations (CPCO) à Paris s'est également modernisé, déménageant de « l'ilot Saint Germain » vers le nouveau ministère de la Défense à Balard, s'accompagnant notamment par la mise en service d'une salle de conduite des opérations, la cellule de veille et de suivi des opérations. Celle-ci est équipée des derniers systèmes de commandement interarmées, permettant la visualisation en direct des forces terrestres déployées

(2) Directives interarmées n° 1 et 3 (DIA-01, DIA-03).

(3) Opération *Épervier* : Tchad, février 1986 à juillet 2014.

(4) Opération *Serval* : Mali, janvier 2013 à juillet 2014.

Commander les opérations en 2030 : quel équilibre entre centralisation réactive et réalités de terrain ?

en Afrique, des avions en mission, des bateaux en patrouille, avec la possibilité de zoomer sur des situations particulières grâce, par exemple, à la transmission d'images des drones survolant les zones d'engagement.

Par ailleurs, sous la pression d'une opinion publique de plus en plus exigeante, relayée par une justice, des médias et des réseaux sociaux très réactifs, le politique s'implique davantage qu'il y a quelques années dans le quotidien des opérations. Le président de la République réunit actuellement son conseil restreint une fois par semaine, lorsque ses prédécesseurs ne le faisaient qu'à quelques rares occasions au cours d'une année. De même, lors du lancement de l'opération *Serval* au Mali, les points de situation sur l'avancée détaillée des forces au profit des autorités politiques pouvaient avoir lieu quotidiennement. Ainsi, le temps court du politique investit toujours plus le temps long du militaire, qui doit maintenant adapter ses méthodes de fonctionnement, vers davantage de réactivité, privilégiant inévitablement la conduite à la planification. Les centres de commandement équipés d'écrans vidéo, de cartes numériques de situation des forces en action et de systèmes de transmission des ordres sous forme de *Chat* ⁽⁵⁾, reliant directement le C2 au combattant, deviennent dans ce contexte des outils particulièrement attirants, tant pour le responsable politique que pour le chef militaire.

Certaines opérations, qualifiées de stratégiques, sont d'ailleurs régulièrement commandées depuis l'échelon militaire parisien, voire depuis l'Élysée. Il s'agit tout d'abord des opérations de dissuasion nucléaire, conduite du Centre des opérations des forces nucléaires (COFN) et contrôlées par l'État-major particulier (EMP), mais également des opérations de ciblage des réseaux terroristes par les forces spéciales, à partir du Commandement des opérations spéciales (COS) à Villacoublay ou des actions de lutte informatique, pilotées depuis Paris. Dans ces trois cas, le plus haut niveau de l'État-major des armées (EMA), en liaison étroite avec la présidence de la République, commande les opérations dans ses phases les plus sensibles.

Ce commandement très centralisé peut-il ainsi se généraliser à l'avenir à l'ensemble des opérations, en France comme sur les théâtres d'opérations extérieures ? L'avènement de nouvelles technologies peut-il conduire à envisager un tel scénario de C2 parisien, en mesure de tout voir et de tout commander à distance ?

Des capacités de combat émergentes dans un monde toujours plus numérique

La capacité militaire qui émerge de façon la plus visible est le drone Male ⁽⁶⁾ de type *Predator* américain, dont l'emploi est maintenant généralisé dans les opérations. La France devrait posséder une douzaine de drones *Reaper* ⁽⁷⁾ dans les années à venir, lui permettant de couvrir quasiment en permanence ses opérations extérieures. Les premiers systèmes sont actuellement mis en œuvre à partir de la base projetée de Niamey

(5) *Chat* : espace numérique de discussion par écrit et en direct.

(6) Male : drone de reconnaissance et de surveillance (Moyenne altitude et longue endurance).

(7) Cf. *Livre blanc sur la Défense et la Sécurité nationale* de 2013.

Commander les opérations en 2030 :
quel équilibre entre centralisation réactive et réalités de terrain ?

au Niger. Mais l'exploitation des vidéos peut se faire à distance à N'Djamena (Poste de commandement de l'opération *Barkhane*), à Lyon (CNOA) voire à Paris (COS, CPCO), déportant ainsi la capacité à décider en direct, en « temps réel » en langage de spécialiste. Alors que l'armement de ces aéronefs est aujourd'hui à l'étude en France, le scénario d'une frappe depuis un système non piloté sur un objectif en zone de combat, décidée par une autorité politique placée devant une vidéo retransmise en direct, à des milliers de kilomètres, semble tout à fait envisageable à court terme en France, à l'image de ce que les Américains pratiquent déjà depuis des années.

De la même façon, des évolutions marquées sont attendues dans le domaine du spatial militaire. La qualité des capteurs photo et vidéo comme de celle des senseurs électromagnétiques devrait être considérablement accrue. L'exploitation de ces nouveaux systèmes – projets *MUSIS* ⁽⁸⁾ et *Ceres* ⁽⁹⁾ – et la concrétisation des projets de surveillance vidéo de la Terre en haute définition (jusqu'à un mètre de résolution) et en temps réel par des satellites géostationnaires – projets *UrtheCast*, *SkyBox*, *GeoEye*, *DigitalGlobe* – multiplieront les sources et la qualité du renseignement, donc accéléreront significativement la boucle décisionnelle du *C2*.

À plus long terme, toujours dans le domaine du renseignement, certains projets innovants ouvrent de nouvelles perspectives dans ce domaine de l'observation permanente du champ de bataille. *Thales Alenia Space* travaille aujourd'hui sur un concept de ballon dirigeable stratosphérique, baptisé *StratoBus* ⁽¹⁰⁾, pouvant couvrir en stationnaire une zone de plusieurs centaines de kilomètres pendant de nombreux mois, à un coût d'exploitation et une complexité de mise en œuvre bien inférieurs à ceux d'un satellite. Cette capacité aura inévitablement une influence sur le fonctionnement des centres de commandement, diminuant les forces de reconnaissance déployées et apportant la persistance de l'image au-dessus des engagements. Autre exemple ouvrant le champ de l'imaginaire dans ce domaine, l'Armée de l'air des États-Unis travaille sur un concept de bombardement depuis l'Espace ⁽¹¹⁾, afin de se libérer de toute empreinte au sol et des contraintes de pénétration des espaces aériens souverains.

D'autres secteurs capacitaires en cours de modernisation s'accompagnent également d'une modification de la fonction de commandement. En France, l'arrivée de l'avion de transport stratégique *A400M* a conduit à centraliser son exploitation, compte tenu de ses capacités logistiques continentales, couvrant plusieurs pays et plusieurs théâtres d'opérations au cours d'une seule mission. Aux États-Unis comme chez certains de nos alliés (de plus en plus nombreux) de l'Otan, la mise en service de l'avion de chasse *F-35* ⁽¹²⁾, plateforme de combat mais également *ISR* (*Intelligence*,

(8) *MUSIS* : *Multinational Space-based Imaging System for Surveillance, Reconnaissance and Observation*, programme de satellite de reconnaissance européen.

(9) *Ceres* : *Capacité d'écoute et de renseignement électromagnétique spatiale*, projet de satellite militaire français de renseignement par écoute électronique.

(10) *StratoBus* : projet de ballon de 100 m de long, stationnaire à 20 000 m d'altitude pour des mois, horizon 2020.

(11) HOUSE Daniel J., TILLER John et RUSHING John, « Suborbital Strike! The Use of Commercial Suborbital Spacecraft for Strike Missions », *Air & Space Power Journal*, vol. 30 n° 4, hiver 2016, p. 46-60.

(12) *F-35* : avion de chasse de dernière génération construit par Lockheed Martin devant équiper les armées américaines (*Air Force*, *Navy* et *Marine Corps*), australienne, canadienne, coréenne, danoise, israélienne, italienne, japonaise, norvégienne, néerlandaise et britannique.

Commander les opérations en 2030 :
quel équilibre entre centralisation réactive et réalités de terrain ?

Surveillance and Reconnaissance) et relais de communications, développant de nouveaux réseaux de communication collaboratifs et réactifs, va entraîner dans son sillage la modernisation des centres de commandement alliés, toujours plus connectés et informés grâce à ces nouveaux systèmes.

Au sol, le programme *Scorpion* ⁽¹³⁾ de l'Armée de terre française va se traduire par la mise en service de véhicules de combat terrestre connectés, en réseau avec des fantassins eux-mêmes individuellement connectés, partageant et transmettant vers les échelons supérieurs une situation tactique permanente, pouvant conduire à une prise en compte en temps réel de la manœuvre par le C2, disposant d'une vision du champ de bataille bien plus complète qu'actuellement.

En mer, tous les bâtiments récents de la Marine nationale sont déjà autant de « plateformes C2 », reliées entre elles et partageant la situation aéromaritime globale les C2 à terre, grâce aux différentes liaisons tactiques L11, L16, L22, dont les potentialités sont infinies.

Dans un futur plus lointain, certaines technologies en cours d'exploration pourraient aussi modifier encore plus profondément ce rapport entre commandement de terrain et C2 :

- les véhicules terrestres autonomes, pilotés à distance, préfigurés par les premiers essais de voitures de tourisme autonomes (Tesla, Uber, Google...) ;
- les robots armés, les soldats augmentés (exosquelette, interface cerveau-machine...) ;
- les nouvelles formes d'énergie, la miniaturisation, donnant allonge et persistance sur le terrain (hydrogène, nanotechnologie...) ;
- l'identification automatique, l'intelligence artificielle ⁽¹⁴⁾, l'informatique quantique, offrant autant de possibilités d'aides au commandement dans les trois milieux.

L'expérience menée par l'Armée de l'air américaine en 2016 de reconnaissance autonome par un essaim d'une centaine de minidrones *Perdrix* ⁽¹⁵⁾, largués par des avions de chasse, illustre encore l'accélération du progrès dans tous ces domaines.

D'une manière plus générale, la généralisation croissante du numérique dans l'ensemble des secteurs d'activité humaine, couplée à l'extension prévisible de la couverture par les réseaux de communications de téléphonie mobile de l'ensemble des zones habitées dans le monde, va multiplier les possibilités de localisation et de communication à bas coût. Ces réseaux constitueront autant de relais ou de moyens de communication dans les zones traditionnelles d'engagement de nos forces (Afrique, Moyen-Orient), aujourd'hui encore peu numérisées. Les perspectives qui en découlent

(13) *Scorpion* : programme de modernisation des capacités de combat de contact, *via* notamment la rénovation du char *Leclerc*, la mise en service de nouveaux véhicules blindés *Griffon* et *Jaguar* ainsi que la mise en réseau de l'ensemble des systèmes terrestres.

(14) En 2016, le robot *Alpha* de la société Psibernetix, développé en partenariat avec l'*US Air Force* et l'Université de Cincinnati, a battu à plusieurs reprises en combat aérien un pilote de chasse très expérimenté.

(15) « Department of Defense Announces Successful Micro-Drone Demonstration », 9 janvier 2017 (www.defense.gov/).

Commander les opérations en 2030 : quel équilibre entre centralisation réactive et réalités de terrain ?

pour le commandement des opérations sont extraordinaires. Par l'intermédiaire d'applications *ad hoc* sur des systèmes militaires dédiés ou trouvés dans l'industrie civile, tout vecteur connecté (soldat, véhicule terrestre, bateau, aéronef, satellite) sera en mesure de dialoguer avec le C2, enrichissant de façon exponentielle les cycles de renseignement et de décision.

La mise en service récente du système de communication et de commandement *Auxylium* ⁽¹⁶⁾ dans l'Armée de terre française constitue une première brique vers cet emploi dual des réseaux civils, au profit des opérations militaires.

Du C2 au C4ISTAR ?

Dans le domaine plus particulier du C2, l'avènement de systèmes de fusion des informations tactiques, du renseignement, des communications, de la simulation et des outils de commandement ainsi que la généralisation du concept de « *Combat Cloud* ⁽¹⁷⁾ » devrait conduire à repenser la place du chef militaire. L'ACT ⁽¹⁸⁾ travaille actuellement sur une réflexion prospective *2030 C2 Vision* sur ce sujet, remplaçant le terme de C2 par celui de C4ISTAR ⁽¹⁹⁾. Douze concepts fonctionnels ⁽²⁰⁾ y sont définis dans quatre domaines, baptisés « *Connecting, Collecting, Decision Making, Effecting* ». Les notions de « *Federation of Cloud* » et de « *Global Information Sphere* » émergent. Sur un plan plus technique voire anecdotique mais symbolique, la visualisation 3D au profit des C2 est évoquée alors que certains industriels travaillent sur des casques immersifs pour le décideur, au cœur du C2. Ce dernier serait ainsi en mesure d'élaborer des ordres très précis et réactifs, construisant sa synthèse de la situation puis ses ordres grâce à la fusion des situations tactiques de tous les échelons déployés. Le général d'armée aérienne Denis Mercier, chef de l'ACT, donne sa vision du C2 en ces termes : « *Achieve synchronized, comprehensive and optimised collective effects, cost efficiencies and zero day mission readiness through a continuous, agile, resilient and force-multiplying capability to unite* ».

Utilisées à bon escient, ces nouvelles technologies de l'information représenteront certainement une avancée considérable dans l'exercice du commandement opérationnel. Les atouts de cette centralisation extrême sont multiples. L'état-major, quel que soit son niveau dans la chaîne hiérarchique bénéficiera, comme nous l'avons vu plus haut, d'une vision globale sur l'ensemble des capacités déployées, lui permettant d'adapter sa manœuvre en conduite, en lien direct avec son niveau supérieur. Il gagnera en réactivité dans l'application des effets mais également dans la capacité à

(16) *Auxylium* : utilisation des services de communication numérique très haut débit civils ou militaires, à partir d'un smartphone, permettant en outre la localisation, le contrôle à distance de robot ou de drone.

(17) *Combat Cloud* : partage de données numériques tactiques, fusionnées dans une banque de donnée.

(18) *ACT* : *Allied Command for Transformation*, commandement de l'Otan en charge de la modernisation des forces, des capacités, des doctrines et des structures.

(19) *C4ISTAR* : *Computerized Command Control Communications Intelligence Surveillance Target Acquisition Reconnaissance*, architecture de systèmes de C2.

(20) *Global ubiquitous communications, federation of clouds, cyber defense, artificial intelligence and sensor edge, cognitive computing, comprehensive awareness, human sensemaking, accelerated decision, distributed decision, federated cyber ops, synchronized effects, artificial intelligence and effector edge.*

Commander les opérations en 2030 : quel équilibre entre centralisation réactive et réalités de terrain ?

communiquer, quasiment en direct sur les événements en cours. Les ordres pourront être simplifiés, plus directs, donc moins sujets aux interprétations ou aux incompréhensions. Le compte rendu sera également immédiat et fidèle, car retranscrit automatiquement et en direct.

Ce modèle répondra parfaitement aux exigences du temps court, politique et médiatique, d'opérations de ciblage, de contre-terrorisme ou de lutte informatique comme nous les connaissons actuellement. Il conviendra en outre aux impératifs de réactivité et de contrôle étroit des opérations de dissuasion nucléaire, de défense antimissile balistique ou de défense aérienne sur le territoire national.

Un commandement très centralisé permettra également de diminuer significativement les effectifs des états-majors, en métropole ou déployés en opérations. Les C2 partageant la même situation numérique des opérations en cours, les outils de communication reliant la métropole au combattant, la structure traditionnelle à trois niveaux stratégique, opératif et tactique ainsi que l'armement en personnel d'état-major pourront être revus. De la même façon, la bascule d'activité de planification vers davantage de conduite pourra permettre de réduire les postes dédiés à la préparation des opérations (renseignement, plans, rédaction des ordres). Les gains seront d'ordre financier, car les effectifs seront moins nombreux et moins engagés. Les risques sur la force déployée seront limités, car moins nombreux et en mesure de commander à distance des zones de contact. Dans un contexte sociétal et politique où l'opinion publique est chaque jour plus réticente à risquer la vie de ses soldats, notamment sur le sol d'un autre pays souverain, ce concept de C2 devient très séduisant.

Des réalités de terrain, un cadre interarmées et interalliés

Si ce commandement à distance procure effectivement de nombreux avantages, il présente en revanche aussi des risques réels sur la réussite des opérations.

La première dérive naturelle du chef au sein d'un C2 moderne sera sa tendance à prendre les décisions à la place des niveaux subordonnés, le général allant jusqu'à décider à la place du combattant de terrain. Vidéo de drone, liaison de données affichant l'ensemble des paramètres du système de combat, main courante des échanges radio, carte numérique du champ de bataille : cette profusion de merveilles technologiques peut en effet donner au commandement une fausse perception du terrain, déconnectée de ses réalités comme la météorologie, le relief, le danger, le moral des combattants, conduisant ainsi le chef à donner des ordres n'étant pas de son niveau, hors de contexte et *in fine* inefficaces voire dangereux.

Les échelons subordonnés, pilotés en boucle courte, pourraient aussi progressivement se désresponsabiliser, perdre leurs expertises tactiques, leurs connaissances des milieux et abandonner toute initiative. Le chef comme les adjoints ne prendraient alors plus suffisamment de recul, abandonnant la stratégie vers des objectifs de long terme aux dépens d'une manœuvre réactive à très court terme.

Commander les opérations en 2030 :
quel équilibre entre centralisation réactive et réalités de terrain ?

Ce modèle centralisé pose en outre la question de la résilience du C2. Reposant excessivement sur des réseaux informatiques et des systèmes de communication comme sur des effectifs comptés et exécutants, un commandement devient très vulnérable face à une attaque cybernétique, au brouillage des réseaux, aux attaques électromagnétiques, aux impulsions électromagnétiques ⁽²¹⁾, aux simples pannes des systèmes de communication embarqués.

Une centralisation abusive concentrerait l'ensemble des opérations sur trop peu de personnes, conduisant à une saturation du commandement. Le Céma, son sous-chef opérations ainsi que le chef du CPCO doivent en effet pouvoir déléguer une part de leurs responsabilités aux commandants de forces et de théâtres, compte tenu du nombre d'opérations engagées par les armées actuellement, sur le territoire national comme à l'étranger. La subsidiarité déclinée dans les trois niveaux prend ici tout son sens.

La ressource humaine que constituent les opérateurs de C2 doit également être prise en considération dans cette problématique. Un C2 en métropole qui conduirait sur une longue durée des opérations à des milliers de kilomètres rencontrerait progressivement des difficultés, liées à la perte de connaissance du théâtre, diluée dans le quotidien ; à la chute de motivation du personnel, engagé en opérations sans l'être, participant virtuellement au combat, sans en retirer le sens du devoir accompli ni la reconnaissance attendue, étant resté très loin du front... sans évoquer la complexité de la formation des opérateurs, par simulation, loin des réalités du combat. Ni la gestion des relèves incessantes d'un personnel finalement peu motivé car voué aux contraintes mais sans les aventures ni les récompenses. Cela constitue aujourd'hui un des enseignements majeurs de l'Armée de l'air après quelques années de pratique du *JFAC AFCO* ⁽²²⁾ « *Full Rear* » de Lyon.

Par ailleurs, des études récentes guidées par cette modernisation en cours, recherchant une rationalisation des C2 et une économie de moyens, ont conduit à remettre en question le niveau opératif. Or il s'agit bien de l'étage clef dans la conduite d'une opération militaire. À l'intersection de tous les acteurs, donneurs d'ordres, exécutants et concourants, il assure la continuité, la cohérence et l'intégration interarmées comme internationale de toutes les forces. De plus, il concentre la connaissance la plus précise du terrain avec la vision stratégique de l'état-major central. Il se nourrit des échanges de proximité, avec les forces déployées comme avec les partenaires des autres nations. L'actuelle structure à trois niveaux reste donc pertinente, malgré les mirages séduisants du C2 du futur.

Des relations humaines de qualité entre combattants partenaires, locaux ou alliés, restent aussi indissociables des opérations, car nécessaires à la bonne compréhension des enjeux locaux et essentielles pour la coordination des forces. Il n'est alors pas envisageable, quelle que soit l'époque, la culture ou la qualité des systèmes de

(21) Impulsion électromagnétique : émission d'ondes électromagnétiques de très forte amplitude qui peut détruire les appareils électroniques et brouiller les télécommunications. Elle peut être provoquée par une bombe spéciale ou une explosion nucléaire.

(22) *JFAC-AFCO* : *Joint Forces Air Command* pour l'Afrique centrale et de l'Ouest, C2 Air de *Barkhane*.

Commander les opérations en 2030 :
quel équilibre entre centralisation réactive et réalités de terrain ?

visioconférence, de construire un rapport de confiance mutuelle à distance. Le vocabulaire militaire de *Key Leader Engagement* ⁽²³⁾ est employé pour décrire ces relations humaines à vocation opérationnelle, entre le commandant opérationnel et ses interlocuteurs locaux. Le chef opératif ou tactique doit donc absolument commander depuis le théâtre d'opération, au contact des politiques de proximité, des diplomates, des représentants des organisations internationales ou non gouvernementales, de la presse locale, des chefs militaires alliés, de ses subordonnés.

Car le commandant d'une opération a également un rôle de chef militaire au contact qui ne peut être délégué. Sa relation étroite avec ses adjoints et ses hommes est un des facteurs clés conduisant à la réussite des missions. Il doit ressentir le moral des troupes, le prendre en compte dans sa stratégie, le construire, le reconstruire et enfin savoir donner à chacun du sens aux missions qu'il ordonne, motiver et montrer l'exemple, afin de disposer de forces toujours plus performantes.

Par ailleurs, la France intervient régulièrement en tant que membre de l'Otan, de l'Union européenne ou comme allié du premier cercle aux côtés des armées américaines. Ainsi, la majorité de ses engagements opérationnels est réalisée en coalition internationale, comme en Irak ⁽²⁴⁾ actuellement. En conséquence, nos états-majors se doivent de maîtriser les organisations et fonctionnements normalisés des C2 de nos partenaires. Trop s'éloigner de la doctrine en la matière conduirait à une perte de compétence de nos experts C2 et des difficultés de coordination à long terme. Un minimum de conservatisme est nécessaire, au moins dans la présentation et la lisibilité de nos organisations.

Enfin, en interne, l'organisation interarmées doit également rester équilibrée et cohérente. Le déport à Lyon de la composante aérienne du commandement de l'opération *Barkhane*, dont le PC opératif est à N'Djamena, est à ce titre régulièrement critiqué. En effet, malgré les liaisons et les échanges nombreux entre les deux C2, l'absence de structure aérienne à N'Djamena complexifie la construction puis la conduite d'une stratégie et d'une manœuvre interarmées.

Cette séparation physique nuit en outre à la visibilité de l'ensemble. Le C2 étant le premier lieu visité par les autorités ou observateurs extérieurs (partenaires, journalistes) lors de leur passage sur un théâtre, la force apparaît amputée d'une de ses composantes. La cohésion interarmées peut en souffrir. La visibilité de l'action d'une armée par rapport à l'autre aussi. L'évolution des structures gagerait donc à avancer de façon progressive et synchronisée en interarmées.

Quel équilibre, quelle place pour le chef, quel outil ?

Quelles seront alors les tendances envisageables pour le C2 dans les années qui viennent, accompagnant la mise en service de nouveaux systèmes militaires ?

(23) *KLE* : travail d'influence des chefs à des fins opérationnelles ou d'approche globale.

(24) *Operation Inherent Resolve*. Pays participants : États-Unis, France, Royaume-Uni, Arabie saoudite, Émirats arabes unis, Pays-Bas, Canada, Australie, Danemark, Maroc, Jordanie, Bahreïn, Qatar et Turquie.

Commander les opérations en 2030 :
quel équilibre entre centralisation réactive et réalités de terrain ?

Tout d'abord, quels que soient les outils et les doctrines, il faut continuer d'être en mesure de commander depuis Paris, notamment au lancement d'une opération, en réactif, suite à un événement soudain, comme cela a pu être le cas au déclenchement de l'opération *Serval* en janvier 2013, afin de stopper l'avancée de la colonne rebelle au Mali vers Bamako. L'armement d'une capacité minimale en systèmes et opérateurs ad hoc en central reste en conséquence pertinent.

Ensuite, en acceptant le progrès sans cependant remettre en question cette architecture traditionnelle de C2 à trois niveaux de commandements, la numération aboutie du champ de bataille et la guerre en réseaux pourraient conduire à une compression des effectifs de ces niveaux, les postes des états-majors opérationnels étant progressivement réduits en parallèle du développement des systèmes toujours plus automatisés. Cette réduction d'effectif devrait également être accentuée par la bascule de charge entre planification et conduite, par l'éventualité de nouvelles formes d'ordres numériques, remplaçant les documents traditionnels en papier, économisant une part de la ressource humaine consacrée à ces tâches. Un modèle d'état-major stratégique bien armé, s'appuyant sur un opératif resserré autour de son chef disposant d'un C2 automatisé et performant, commandant suivant un cycle accéléré à des niveaux tactiques encore plus réduits, en conduite sur court préavis vers des forces connectées, peut être envisagé.

Deux approches sont possibles dans cette réflexion sur l'évolution du C2 dans les années à venir. D'un côté, on trouve une vision prudente d'experts, s'appuyant sur des expériences vécues de dérive du chef ne maîtrisant pas ce nouvel environnement du C2, saturé d'informations et d'images, tombant dans le piège du « *micromanagement* ». Cette perception pourrait se résumer par cette phrase entendue à plusieurs reprises « la technologie brouille les périmètres du commandement ».

De l'autre, une vision comme celle portée par l'ACT, plus prospective et peut-être plus exaltée par l'accélération du progrès numérique, encourage une modernisation significative du C2 et des processus de commandement des opérations, redonnant paradoxalement au chef militaire toute sa valeur dans le dispositif. « Si la perfection des machines ne peut manquer d'accentuer le caractère technique de la guerre, [...] elle fera reparaître dans l'exercice du commandement certaines conditions de hâte et d'audace qui rendront tout son relief à la personnalité ». Cette citation de Charles de Gaulle (*Vers l'armée de métier*, 1934) donnerait-elle raison aux officiers de l'Otan ? Le développement du C2 ne conduit-il pas inexorablement le chef à se placer au cœur du système, comme le préfigure le commandant d'un bâtiment de combat moderne⁽²⁵⁾, ayant déserté la passerelle pour le central opérations, à la manœuvre face à une multitude d'écrans numériques.

Qui donc doit décider ? Et où, en central ou sur le terrain ? Quelle que soit la bonne orientation, il apparaît incontournable d'anticiper la complexité de l'exploitation de ce nouvel environnement et de travailler sur la formation du décideur au

(25) *Frégates multi-missions (Fremm)* de type « Aquitaine », frégates anti-aériennes de type « Horizon », *Bâtiments de projection et de commandement (BPC)* de type « Mistral ».

Commander les opérations en 2030 :
quel équilibre entre centralisation réactive et réalités de terrain ?

commandement au sein d'un C2 moderne. Au-delà de l'apprentissage à l'emploi des nouvelles technologies, il convient de le préparer à la réflexion dans un environnement surchargé d'information, créé par la numérisation. Il doit être préparé à trouver un équilibre entre le renseignement numérique et le renseignement de terrain, vers une prise de décision rapide et sûre. La simulation intégrée dans les systèmes de commandement apportera à ce titre une grande plus-value. Et la pensée du Maréchal de Lattre méritera peut-être un jour d'être inscrite aux murs des C2, dominant les travées d'écrans : « Un outil ne vaut que par la main qui l'anime ».

Il conviendra aussi de concrétiser la mise en cohérence de tous les systèmes de commandement. En effet, chaque armée, chaque pays, chaque alliance internationale, chaque milieu, a développé au fil de ces dernières années les logiciels correspondant à ses besoins de planification, de conduite et de contrôle ⁽²⁶⁾. Afin de bénéficier de la synthèse de l'ensemble des systèmes, vers un C2 performant, un programme d'ensemble devra fusionner l'ensemble des systèmes. Il s'agit d'un enjeu technique et politique majeur, en raison des contraintes de transmission en temps réel des données, de comptabilité de dialogue, des règles de confidentialité et des rivalités industrielles. Le programme SIA ⁽²⁷⁾ constitue une première étape. L'ACCS ⁽²⁸⁾ de l'Otan est également une démonstration encourageante d'un système fusionné au niveau international. Les étapes suivantes devront réussir à fédérer les trois milieux terre, air, mer et faire partager aux trois niveaux de commandement la même situation tactique en temps réel.

Conclusion

Au XIX^e siècle, l'empereur Napoléon Bonaparte commandait lui-même ses armées, sur le terrain, au cœur des batailles. En mai 1940, l'*Air Marshal Dowding* gagnait la bataille d'Angleterre depuis son *bunker* d'Uxbridge au Nord-Ouest de Londres, construisant une vision centralisée des opérations aériennes à partir de dômes de bois représentant des formations d'aéronefs, déplacées en temps réel par des opératrices sur une grande carte déployée. Aujourd'hui les liaisons de données rendent compte de façon instantanée des positions des systèmes d'armes connectés, au PC de *Barkhane* à N'Djamena ou au CPCO à Paris.

Demain, comme nous l'avons vu ci-dessus, l'augmentation exponentielle de la robotisation et de la numérisation transformeront encore l'art de conduire les opérations. Grâce à la technologie, la connaissance par le chef de l'état des forces et de la situation instantanée – *situation awareness* – sera encore considérablement augmentée, accélérant le cycle de décision et élargissant le champ des options militaires, augmentant en conséquence le rythme des ordres vers les échelons subordonnés.

Cette évolution devrait conduire : à une compression des échelons de commandement à tous les niveaux, la technologie se substituant progressivement à l'homme ; à une diminution de la planification vers davantage de conduite et de tempo

(26) RIFAN, SIC21, FrOps, SICF, ATLAS, SIR, STRIDA, ACCS...

(27) SIA : Système d'information des armées, programme de convergence des systèmes de commandement des armées.

(28) ACCS : Système de commandement et de contrôle aérien de l'Otan.

Commander les opérations en 2030 :
quel équilibre entre centralisation réactive et réalités de terrain ?

dans les opérations, répondant ainsi au fonctionnement des décideurs et opinions ; à une exigence accrue de réactivité et de fugacité des forces, propre à orienter les choix capacitaires et les modes d'actions, vers une manœuvre plus coordonnée, plus étendue et plus fluide ; à une centralisation plus régulière du commandement des opérations, aux dépens de la subsidiarité.

La transformation des armées étant nécessairement liée à celle du monde civil et de nos partenaires militaires, la doctrine interarmées en matière de C2 devra accompagner ces changements, pour trouver un compromis entre technologie et doctrine, entre le C4ISR et les principes de la guerre ! Comme nous l'enseigne Sun Tzu dans *L'art de la guerre*, « si nous voulons que la gloire et les succès accompagnent nos armes, nous ne devons jamais perdre de vue : la doctrine, le temps, l'espace, le commandement et la discipline ». La formation du commandant d'opération de demain, la construction de ses outils, la souplesse des structures et le développement du C2 lui-même comme système de combat constituent dès lors les enjeux de nos réussites opérationnelles de demain.

Commander les opérations en 2030 : quel équilibre entre centralisation réactive et réalités de terrain ?

Éléments de bibliographie

ACT, *NATO NEC C2 maturity model*, février 2010, 186 pages.

ASCENSIO Michel, « Le C2 et la défense antimissile balistique européenne en 2009 », *Recherches & Documents* n°10, Fondation pour la recherche stratégique (FRS), octobre 2010.

BOREL Jean-Jacques (Général de corps aérien, commandant de la défense et des opérations aériennes 2014-2016), « Commander et conduire les opérations aériennes depuis la métropole : plus-value du *reachback* », *Penser les ailes françaises* n° 34, octobre 2016 (www.cerpa.air.defense.gouv.fr/images/pdf/Plaf/plaf_34.pdf).

CENTRE INTERARMÉES DE CONCEPTS, DE DOCTRINES ET D'EXPÉRIMENTATIONS (CICDE), *Doctrines interarmées DIA-01* (www.cicde.defense.gouv.fr/IMG/pdf/20140612_np_cicde_dia-01-def.pdf) et *DIA-03*.

CUMMINGS Mary. L., *Artificial Intelligence and the Future of Warfare*, Chatham House, 26 janvier 2017 (www.chathamhouse.org/publication/artificial-intelligence-and-future-warfare).

COSQUER Christian, *Les centres de commandement et de contrôle (C2), un enjeu stratégique structurant*, CEIS, 8 septembre 2014 (<https://ceis.eu/>).

DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA), *Document de présentation de la S&T 2014-2019*, 38 pages (www.ixarm.com/IMG/pdf/post_dga_2014_2019.pdf).

GOETZ Pierre et CAHUZAC-SOAVE Olivia, « Impact de la numérisation sur l'exercice du commandement », *Les notes stratégiques du CEIS*, décembre 2015, 32 pages.

GROS Philippe, VILBOUX Nicole, KOVACS Anne, COSTE Frédéric et KLEIN Michel, « Du *network-centric* à la stabilisation : émergence des « nouveaux » concepts et innovation militaire », *Études de l'Irsem* n° 6, 2010 (www.defense.gouv.fr/content/download/153073/1551180/file/Etuden%C2%B06%20-%202010.pdf).

« Les opérations militaires du futur » in *Histoire & Stratégie* n° 18.

HOUSE Daniel J., TILLER John et RUSHING John, « Suborbital Strike! The Use of Commercial Suborbital Spacecraft for Strike Missions », *Air & Space Power Journal*, vol. 30 n° 4, hiver 2016, p. 46-60 (www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-30_Issue-4/F-House_et_al.pdf).

« Le soldat augmenté » (dossier) in *Inflexions* n° 32.

Joint Operating Environment (JOE 2035), The Joint Force in a Contested and Disordered World, 14 juillet 2016 (www.dtic.mil/doctrine/concepts/joe/joe_2035_july16.pdf).

LEONHARD Robert R., BUCHANAN Thomas H., HILLMAN James L., NOLEN John M. et GALPIN Timothy J., « A concept for Command and Control », *Johns Hopkins APL technical digest*, vol. 29 n° 2, 2010, p. 157-170.

LORD Lance W. (général), *Commander le futur*, US Air Force.

MALIS Christian, *Guerre et Stratégie au XXI^e siècle*, Fayard, 2014, 352 pages.

METMATI Djammel, *Stratégie et réseaux dans la conduite des opérations militaires*, 10 janvier 2015.

Entretiens

- Général de division aérienne Jean-François FERLET, chef du Centre de planification et de conduite des opérations (CPCO).
- Général de division Patrick BRETTHOUS, commandant de l'opération *Barkhane* 2015-2016.
- Général de division Xavier DE WOILLEMONT, commandant de l'opération *Barkhane* 2016-2017.
- Colonel Olivier MAURER, commandant en second du Centre national des opérations aériennes (CNOA).
- Colonel Jean-Paul BESSE, chef d'état-major de l'opération *Barkhane* 2016-2017.
- Colonel Louis PENA, chef d'état-major du Commandement pour les opérations interarmées (CPOIA).
- Colonel Philippe COUSSIEU, officier de cohérence opérationnelle « commandement et maîtrise de l'information », État-major des armées.

Quelles orientations face au déni d'accès à l'horizon 2025 ?

Bruno FOUSSARD

| Colonel (air), auditeur de la 66^e session du CHEM.

Compte tenu de ses ambitions stratégiques, de ses intérêts globaux et de son passé expéditionnaire, la France cherche à maintenir ses capacités de projection de puissance et de forces sur l'ensemble du spectre des menaces. La crédibilité de la dissuasion nucléaire, la liberté d'accès aux espaces communs, la présence de nombreux ressortissants français de par le monde et la protection de nos territoires outre-mer sont autant de raisons qui motivent la France à maintenir des capacités d'intervention globales, de manière autonome ou en coalition. Cependant, la prolifération d'une vaste panoplie de moyens de défense active et de systèmes d'armes modernes exploitant des technologies de pointe pourrait présenter une menace sur les modes d'actions employés ces vingt-cinq dernières années.

L'objectif de ce travail est ainsi de comprendre dans quelle mesure les concepts de déni d'accès impactent les ambitions et les capacités expéditionnaires françaises et d'étudier quelles pourraient être les stratégies qui permettraient d'en limiter les effets sur nos modes d'actions à l'horizon 2025.

Ces concepts de déni d'accès, s'ils ne sont pas nouveaux, compliquent voire empêchent l'accès à des zones de déploiement sanctuarisées, sur lesquels les armées modernes ont appris à compter depuis l'opération *Desert Storm*. Marquant la fin d'une parenthèse de près de trente ans, ils mettent en danger à moyen terme la capacité des forces militaires occidentales à entrer en premier et à opérer en toute impunité dans des milieux permissifs.

La notion de déni d'accès, traduite du concept américain d'*Anti-Access/Area Denial (A2AD)* est de plus en plus fréquemment utilisée dans la rhétorique de défense, tout en étant souvent comprise seulement de manière partielle. Dans une première partie, ce travail montrera que le concept de déni d'accès s'applique à l'ensemble du spectre des capacités, et qu'il a des implications stratégiques sur l'ensemble de nos forces et de nos ambitions politiques. Par ailleurs, si ce concept a souvent fait l'objet de réflexions, il ne se traduit pas aujourd'hui par une prise en compte réelle en termes doctrinaux, capacitaires, organisationnels. Cette étude proposera en seconde partie des orientations pragmatiques, s'inscrivant dans un horizon contraint ne permettant pas de remédier à cette problématique par des solutions programmatiques.

De la liberté d'action à la contestation des modes d'action expéditionnaires

L'expression de la souveraineté et des ambitions françaises

L'héritage expéditionnaire de la France et l'autonomie stratégique, confirmés par le Livre blanc sur la Défense et la Sécurité nationale 2013

La capacité à déployer des forces et à entrer en premier tient une place essentielle dans la politique de défense de la France, pour des raisons historiques, politiques et militaires renvoyant notamment à l'ambition nationale d'autonomie stratégique. Depuis la Seconde Guerre mondiale, la France a été impliquée dans un grand nombre d'opérations loin de ses frontières, en coalition ou en totale autonomie.

La IV^e République voit ainsi l'engagement de ses forces dans la guerre d'Indochine dès 1946, en Corée en 1950 et en Algérie de 1954 à 1962. L'intervention de Suez en octobre 1956 aux côtés des Britanniques démontre la supériorité des capacités de projection de moyens modernes de combat de haute intensité. Elle montre également la volonté française de disposer d'une autonomie stratégique pour intervenir seule lorsque ses intérêts vitaux sont menacés. Durant la V^e République, en plus de diverses crises de moyenne intensité, la France participera à partir de 1990 à plusieurs conflits coalisés majeurs et structurants : guerre du Golfe, interventions au Kosovo et en Afghanistan, opérations en Lybie, en Syrie et dans la Bande sahélo-saharienne (BSS). Au cours de ces opérations récentes, la France a ainsi démontré qu'elle possédait des savoir-faire et des capacités de projection de forces et de puissance rares, voire uniques en Europe, qui lui ont offert une liberté d'action extérieure considérable et un fort levier pour l'action multinationale.

Le *Livre blanc 2013* conforte ces ambitions sans ambiguïté, dans la continuité des revues stratégiques précédentes. Il note en particulier : « La France entend disposer des capacités militaires lui permettant de s'engager dans les zones prioritaires pour sa défense et sa sécurité : la périphérie européenne, le bassin méditerranéen, une partie de l'Afrique – du Sahel à l'Afrique équatoriale –, le golfe Arabo-Persique et l'océan Indien. [...] [Dans ces zones,] [...] nos forces devront pouvoir être engagées dans une opération de coercition majeure, [...], dans un contexte de combats de haute intensité. [...] À ce titre, les forces françaises conserveront la capacité de participer à une opération d'entrée en premier sur un théâtre de guerre dans les trois milieux. »⁽¹⁾ Par ces éléments, il souligne d'une part l'étendue des zones d'engagement potentielles de la France, qui imposent des capacités de projection robustes et qui présupposent une aptitude à instaurer des points d'appui à proximité de théâtres d'opérations en vue d'y conduire des actions militaires dans la durée ; d'autre part, il note le besoin d'une capacité d'entrée en premier reposant sur une liberté d'action dans les trois milieux, même temporelle et locale, alors même qu'il dresse le constat que les « risques et les menaces auxquels la Nation doit faire face se sont multipliés en se diversifiant »⁽²⁾. Ainsi, le *Livre blanc 2013* confirme les ambitions de la France pour les dix années à venir en insistant

(1) *Livre blanc 2013*, p. 82 et 92.

(2) *Ibid.*, p. 10.

sur le maintien d'une « capacité autonome à “entrer en premier” sur un théâtre d'opérations de guerre. »⁽³⁾.

Ce sont effectivement ces capacités qui permettront à moyen terme de continuer à jouir d'un certain niveau de supériorité technologique pour conduire les opérations dans des environnements de moins en moins permissifs. Mais elles ne suffisent pas pour garantir le déploiement de forces en vue de mener des opérations.

La fin d'une parenthèse de vingt-cinq ans

Depuis la première guerre du Golfe, les armées occidentales ont en effet pu jouir d'une totale supériorité dans les trois milieux, principalement apportée par nos alliés américains, leur permettant d'établir des points d'appui afin de projeter des effets sur l'adversaire dans la durée. Cette domination occidentale des années 1990-2000, accompagnée par une passivité initialement résignée des adversaires, a conforté la France et ses alliés dans une fausse certitude de supériorité durable. Nos modes d'actions n'ont ainsi que très peu évolué depuis des décennies, dans la croyance que la conservation de la maîtrise des milieux de combat garantirait longtemps notre capacité à nous déployer et à conduire des opérations loin de nos frontières.

Pourtant, durant ces années de maîtrise incontestée des milieux, nos adversaires se sont adaptés et ont démontré que nos modes actions, essentiellement basés sur la supériorité technologique, étaient vulnérables. En l'occurrence, la première réponse du faible au fort observée à partir du deuxième conflit en Irak et durant le conflit en Afghanistan aura été le combat asymétrique, qui commença à exploiter les vulnérabilités de nos modes d'action en réduisant les écarts permis par la technologie. En utilisant les moyens de communication modernes, les explosifs improvisés (IED) sur nos troupes projetées, les techniques de guérillas et de harcèlement en se mêlant aux populations et aux environnements urbains, ces adversaires ont montré que cette parenthèse de supériorité incontestée des Occidentaux touchait à sa fin.

Le retour des puissances

Le deuxième phénomène qui sonne le glas de cette supériorité est lié au retour à la confrontation des puissances et au retour de la force, comme le souligne le *Livre blanc 2013*.

Avec l'arrivée au pouvoir de Vladimir Poutine (1999), la réaffirmation de la puissance russe dans son environnement proche se traduit par un réarmement massif, des postures, des attitudes provocatrices et l'utilisation de « proxis » qui permettent la prolifération de stratégies de dénis d'accès. Les enjeux stratégiques relatifs aux espaces communs relèvent de cette politique, justifiée par la Russie comme étant issue de la menace que la politique des États-Unis dans son environnement proche fait peser sur sa sécurité nationale. À partir de cette évaluation stratégique, la Russie adopte ainsi des mesures de renforcement des capacités militaires déployées dans les espaces communs ainsi qu'une stratégie de déni d'accès, que ce soit sur le plan conventionnel ou sur celui

(3) *Ibid.*, p. 139.

de la dissuasion. De même la Chine ne cache pas sa préoccupation stratégique relative à la protection de certains espaces et à leur accès. Cette préoccupation se décline par un discours volontariste, un réarmement accéléré et une politique de prolifération de systèmes d'armes sur l'ensemble du spectre ⁽⁴⁾.

La prolifération générée par le réarmement de la Russie et de la Chine permet davantage aujourd'hui à de nombreux adversaires potentiels d'avoir accès tout autant à des technologies nivelantes du bas du spectre qu'à des systèmes d'armes modernes qui permettent déjà de contester la supériorité occidentale. La montée en puissance de ces deux pays sert ainsi tant leur intérêt national et leur politique étrangère que celui d'États hostiles qui bénéficient des transferts technologiques et des savoir-faire associés et ne veulent plus se laisser dicter les politiques occidentales. En l'occurrence, l'exemple de l'Algérie est représentatif, même s'il n'est pas unique (cf. Annexe I). La hausse des investissements de défense dans les pays des Proche et Moyen-Orient atteste de l'élévation générale des niveaux de menace sur nos forces (cf. Annexe III).

Du déni d'accès stratégique au déni de zone

Ainsi, la prolifération d'une vaste panoplie de défenses actives limitera à moyen terme la capacité des forces militaires occidentales à se déployer et à opérer en toute impunité, comme cela a été le cas dans les précédents conflits. Défense du faible au fort, les moyens de déni de zone s'étendent des armements rustiques bas coûts du type *G-RAMM* ⁽⁵⁾ (cf. Annexe II) aux systèmes sophistiqués tels que les missiles balistiques anti-porte-avions ou les missiles sol-air à long rayon d'action et offrent une résistance potentielle de taille à nos forces expéditionnaires dans l'avenir, comme le souligne le *Livre blanc 2013* : « La diffusion des technologies qui accompagne la mondialisation a d'importantes implications pour l'évolution des menaces. [...] À un niveau intermédiaire, elle peut se traduire par l'acquisition de systèmes d'armes performants par des puissances de second rang mais aussi par des groupes non étatiques, comme ce fut le cas des missiles utilisés par le *Hezbollah* contre un navire israélien. Au niveau le plus élevé, elle peut faciliter la prolifération balistique et celle d'armes de destruction massive » ⁽⁶⁾.

La notion de déni d'accès ⁽⁷⁾ est fréquemment utilisée dans la rhétorique militaire. Ce terme est parfois utilisé malencontreusement, dans la mesure où il n'en existe pas de définition agréée dans le corpus doctrinal français. Il mérite avant tout d'être clairement explicité dans ses deux acceptions : le déni d'accès stratégique et le déni de zone.

Le déni d'accès stratégique et la projection de forces

Des définitions existantes dans la doctrine américaine, celle du *Joint Operational Access Concept* de 2012 est la plus explicite : « *Any action that has the effect of slowing deployment of friendly forces into a theater, preventing forces from operating from*

(4) RAMEL Frédéric, « Accès aux espaces communs et grandes stratégies : vers un nouveau jeu mondial », *Études de l'Irsem* n° 30, 2014.

(5) *Guided Rocket, Ammunition, Mortar, Missiles*.

(6) *Livre blanc 2013*, p. 42-43.

(7) Traduction de l'acronyme américain *Anti-Access – Area Denial (A2AD)*.

certain locations with the theater, or causing forces to operate from distances farther from the locus of the conflict than they would otherwise prefer. »⁽⁸⁾. En l'occurrence, le déni d'accès stratégique se traduit essentiellement par la capacité d'un adversaire à tenir des forces expéditionnaires à distance et à compliquer leur regroupement logistique en vue de ralentir de potentielles opérations d'ampleur. Cette posture relève souvent du niveau politico-stratégique avec l'objectif d'entraver les capacités d'un adversaire à accéder au théâtre lui-même, mais peut également être pertinente au niveau tactique et en basse intensité.

Sur le bas du spectre des menaces, un facteur nouveau lié à la prolifération des technologies duales et des systèmes d'armes modernes bas coût ajoute en effet à la complexité de la situation. Face à des adversaires mieux équipés, une force expéditionnaire peut également se trouver confrontée à des menaces de type *MRBM*⁽⁹⁾. Qu'elles visent des cibles terrestres ou maritimes, ces menaces sont considérées comme anti-accès. Dans le haut du spectre, les domaines maritimes et aériens sont particulièrement menacés par la prolifération de systèmes d'armes russes ou chinois de plus en plus performants et accessibles. Le missile balistique anti-navire chinois *DF-21D*, équipé d'une charge classique, est l'arme la plus récente de sa catégorie, avec une portée de près de 1 500 km. De même, le positionnement choisi de systèmes de défense sol-air longue portée peut compliquer les transits et les flux logistiques aériens, en présentant une menace permanente sur les moyens de transport stratégiques (cf. Annexe IV).

Ces capacités militaires ne doivent pour autant pas faire oublier que les stratégies de déni d'accès stratégique peuvent se décliner plus subtilement. Les pressions diplomatiques et politiques exercées par un adversaire sur un pays éventuellement enclin à accueillir le déploiement de nos forces peuvent être considérées comme une stratégie d'anti-accès. De même, la pression qu'un État pourrait indirectement exercer sur la France par l'intermédiaire de binationaux ou d'une population suffisante de nationaux installés sur le territoire, ne doit pas être sous-estimée. Par la déstabilisation pilotée du pouvoir, le risque de désagrégement de la cohésion nationale, voire de guerre civile, un État pourrait ainsi dissuader une intervention française par une menace directe sur nos intérêts vitaux, si cette intervention n'est pas pleinement assumée et justifiée. Ces modes d'actions peuvent être considérés comme du déni d'accès stratégique et soulèvent un facteur essentiel : la motivation de nos engagements, leur justification et leur légitimité.

Enfin, des attaques informatiques sur un système logistique, sur les moyens de communication, peuvent également rentrer dans cette catégorie. Ce point sera abordé ci-après.

L'entrée en premier et le déni de zone

Si la projection de force est menacée, notre aptitude à entrer en premier sur un théâtre d'opération, puis de produire dans la durée des effets dans un environnement

(8) Toute action qui a pour effet de ralentir le déploiement de forces amies sur un théâtre, en empêchant les forces d'opérer à partir des zones de déploiement idéales ou en obligeant les forces à opérer à des distances plus éloignées de la zone de conflit.

(9) *Medium Range Ballistic Missile* – missiles balistiques moyenne portée à la portée maximale de 1 000 à 1 300 km selon le *National Air and Space Intelligence Center (USA)*.

non permissif sont contraints par les capacités de déni de zone. La doctrine américaine définit le déni de zone ainsi : « *Area denial operations aim to prevent friendly forces freedom of action in the more narrow confines of the area under the enemy's direct control.* »⁽¹⁰⁾. L'objectif de l'adversaire est alors de contraindre ou d'entraver la liberté de mouvement des forces d'intervention en la contestant dans les trois milieux. Typiquement, une défense aérienne intégrée performante, reposant sur des systèmes sol/air évolués, des armements balistiques antirsurface, est considérée comme faisant partie d'une stratégie de déni de zone. Tout armement courte ou moyenne portée permettant de cibler avec précision des forces ennemies, qu'elles soient terrestres, maritimes ou aériennes, menaçant directement l'intégrité d'un territoire, rentre également dans cette catégorie.

Si ces capacités de déni de zone n'interdisent pas l'intervention, elles augmentent significativement le niveau de risque sur nos forces et nous imposent un environnement contesté dans lequel nos troupes n'auront pas la liberté de manœuvre dont elles jouissent depuis vingt-cinq ans. Par ailleurs, il ne sera bientôt plus certain que les opérations d'entrée en premier, phase de plus haute intensité dans un conflit, permettront d'atteindre la maîtrise des trois milieux dans la durée, notamment par l'acquisition d'une supériorité aérienne totale dans l'espace et le temps. Si la supériorité technologique occidentale permet encore de mener, sur une courte période, un effort intense de déstructuration des principales défenses adverses, la densité des défenses et les performances modernes des systèmes d'armes proliférants imposeront probablement de n'accepter que des poches temporaires de supériorité locales et augmenteront notablement la durée des opérations pour atteindre les objectifs militaires.

Les nouveaux espaces contestés

À la contestation de la supériorité dans les milieux traditionnels d'opération s'ajoute celle de milieux nouveaux mais non moins vulnérables, dont les forces modernes sont de plus en plus dépendantes : l'espace et le cyber.

L'espace, milieu de souveraineté

Comme le souligne le *Livre blanc 2013*, « L'espace extra-atmosphérique est devenu indispensable au fonctionnement de services essentiels. Dans le domaine militaire, le libre accès et l'utilisation de l'Espace sont des conditions de notre autonomie stratégique. [...] Les possibilités d'agression dans l'espace augmentent avec les progrès des armes antisatellites, en particulier pour les satellites en orbite basse »⁽¹¹⁾. Les capacités spatiales sont devenues des outils de souveraineté contribuant à l'autonomie nationale d'analyse, de décision et d'action. Elles sont aujourd'hui essentielles pour la France pour fournir un appui indispensable aux opérations en matière de télécommunication, de surveillance et de géolocalisation. Un déni d'accès dans le domaine spatial porterait fortement atteinte à nos capacités de déploiement et d'intervention hors de nos frontières.

(10) Les opérations de déni de zone visent à empêcher la liberté de mouvement des forces amies dans les parties plus confinées de la zone sous le contrôle direct de l'ennemi.

(11) *Livre blanc 2013*, p. 45.

À ce jour, seules de grandes puissances capables de mener des opérations maîtrisées dans l'Espace sont en mesure de faire peser une menace directe sur nos satellites militaires ou duaux, et justifient une surveillance constante de l'Espace. Plusieurs événements ont montré l'aptitude de la Russie et de la Chine à neutraliser les moyens satellitaires par impact direct ou masquage. Si d'autres puissances développent des compétences dans le domaine spatial, l'absence de maîtrise des effets collatéraux liés à la destruction d'un satellite limite ces modes d'actions à un nombre très limité d'acteurs dans les dix ans à venir.

Pour autant, le déni d'accès potentiel à l'Espace ne s'arrête pas à ces types de technologies du haut du spectre et reste à la portée d'États plus modestes militairement, voire d'individus plus difficilement identifiables. Une composante spatiale est en effet constituée d'infrastructures au sol, de lanceur, et *in fine* de moyens de communication pour transmettre les informations recueillies. Il reste donc envisageable de nier l'accès à l'Espace par l'attaque directe de ces infrastructures, par exemple par des actions terroristes ou par une action interne malveillante. Enfin, le brouillage reste la menace la plus simple à mettre en œuvre sans nécessiter des capacités de haut du spectre, notamment concernant le système *GPS* (*Global Positioning System*), particulièrement vulnérable.

Le cyber, un milieu paradoxal

Paradoxalement, le domaine cyber est largement accessible et particulièrement contesté. La cyber criminalité exploite ce domaine à des fins d'escroquerie, de trafic, et minimise les risques en agissant à distance. Certains États mènent déjà des attaques constantes sur nos administrations, nos industries, pouvant impacter la sécurité nationale. Le numérique a complètement envahi nos structures de production d'énergie, de distribution d'eau, de mécanique, de transport, toutes très interconnectés pour des raisons d'efficacité, ouvrant la voie à de possibles actions destructrices aux impacts graves sur les populations. Ce domaine est devenu au cours de la dernière décennie un espace d'affrontement, dans lequel l'attribution des attaques est extrêmement complexe, et qui démultiplie les effets des actions traditionnelles.

Le cyber pourrait ainsi mettre en danger des éléments fondamentaux de nos opérations : les communications, les transmissions de données, les chaînes logistiques, les systèmes de navigation. Outre des attaques indirectes sur ces moyens essentiels, les attaques informatiques peuvent aussi menacer nos moyens de projection de puissance, par des attaques directes ou indirectes. Nos moyens de combat sont en effet vulnérables aux sabotages informatiques à l'occasion de maintenances longues réalisées par des industriels employant des milliers de salariés plus ou moins contrôlés. La complexité de ces systèmes d'armes modernes rend particulièrement difficile la détection d'actes de malveillances qui pourraient ensuite offrir des portes dérobées pour faciliter des attaques cyber au moment opportun pour nos adversaires potentiels. Enfin, la combinaison d'attaques informatiques et de guerre électronique pourrait perturber notablement nos moyens de combat en réduisant leur efficacité ou en les rendant inopérants. Dans tous les cas, la combinaison des moyens traditionnels et des attaques cyber ne fera

Quelles orientations face au déni d'accès à l'horizon 2025 ?

qu'amplifier la portée des stratégies de dénis d'accès, tant au niveau stratégique que tactique.

*
**

Le fait que les capacités de projection de force et de puissance soient aujourd'hui menacées est ainsi une réalité, dans tous les milieux, sur l'ensemble du spectre. Les modes d'action expéditionnaires, tels que les puissances occidentales les conduisent depuis des décennies sans résistance, sont par conséquent compromis à court terme. Les menaces auxquelles nous devons faire face dans les conflits à venir ne peuvent être seulement contrecarrées par la supériorité technologique, longtemps réservée aux puissances occidentales. À un horizon d'une dizaine d'années, des voies d'améliorations sont pourtant envisageables pour conserver notre liberté d'action et réduire l'aptitude de nos adversaires à exploiter ces stratégies de déni d'accès.

Quelles orientations pour conserver notre liberté d'action ?

Les concepts de déni d'accès ne sont pas nouveaux. Les armées ont toujours cherché à identifier leurs ennemis au plus loin et à les frapper avec le moins de risque possible pour leurs propres troupes. À mesure que les technologies ont évolué, les tactiques se sont adaptées pour réagir et exploiter les failles adverses. Ces concepts sont ainsi trop souvent considérés comme un fait accompli. Cet état de fait pourrait amener à concevoir que les moyens actuels ne peuvent pénétrer ou opérer dans un environnement non permissif et hostile. La réponse aux défis posés par les différentes stratégies de déni d'accès est nécessairement globale et ne peut se réduire à des solutions capacitaires.

Garantir l'accès stratégique

« Dans un environnement anti-accès où l'ennemi dispose d'un réseau de bataille crédible capable de délivrer des armements guidés en masse, la phase initiale de toute opération d'entrée sur le théâtre nécessitera d'obtenir la supériorité globale dans tous les espaces de combat. Cela signifie que ce type d'opération sera délibéré et prendra du temps à mettre en oeuvre. Cela ne veut pas dire : "zut ! Des *G-RAMM* ! En avant toute !". Mais plutôt : "Prenez votre temps, éliminez la menace *G-RAMM*, puis déployez-vous dans la zone de votre choix quand vous le déciderez". Pas de débarquement précipité dans ce type d'environnement... Et toute entrée sur le théâtre sera le fruit d'un effort interarmées, qui s'appuiera sur les opérations aériennes et spatiales » ⁽¹²⁾

Des stratégies d'alliance renouvelées

Le prépositionnement des forces françaises présente un intérêt stratégique majeur face aux stratégies d'anti-accès. Nos liens privilégiés avec certains pays d'Afrique

(12) Robert WORK (secrétaire d'État à la Marine américaine) et lieutenant-colonel F.G. HOFFMAN, « Hitting the Beach in the 21st Century », *Proceedings*, US Naval Institute, novembre 2010.

et du Moyen-Orient notamment assurent l'accès à des régions pivots et permettent de soutenir la projection d'une opération dans l'arc de crise potentiel. Ces prépositionnements sont des atouts non négligeables dans une coalition afin de tirer au mieux parti des plateformes utilisables pour établir une posture de forces pertinente et efficace. La connaissance du terrain et des cultures est un facteur déterminant à la réussite d'une projection. À cet égard, la tenue d'une base de données considérant les aspects de soutien, d'avitaillement logistique devient primordiale pour faciliter la planification dans la phase initiale d'une opération. Cet aspect impose toutefois au préalable un important effort diplomatique à l'attention de nos partenaires visant à en faire bénéficier les forces coalisées si besoin.

À plus long terme, l'acquisition de moyens performants afin de garantir notre supériorité technologique restera indispensable dans les opérations menées en coalition. En effet, si seuls les États-Unis affichent encore des capacités inégalées sur l'ensemble du spectre et des concepts d'emplois novateurs (cf. Annexe V), La France n'a pas encore doctrinalement pris en compte le déni d'accès et possède des capacités restreintes en matière de furtivité et de bombardement à long rayon d'action, très en deçà de celles des États-Unis. Un décalage trop important en termes de capacités et de doctrines peut tendre à réduire le rôle des alliés à une portion congrue. Par ailleurs, la tendance actuelle de l'administration américaine de n'offrir que du support à ses alliés, sans fournir de moyens réellement offensifs et sans prendre le lead des opérations, du moins lorsque ses intérêts vitaux ne sont pas menacés, doit inciter la France à se doter de moyens d'opérer d'une manière autonome et à choisir des alliés disposant également de ces capacités.

La protection des forces projetées

Du fait de leur précision, les G-RAMM peuvent avoir des effets disproportionnés. Des acteurs non-étatiques ou des insurgés pourront demain frapper des cibles à forte plus-value avec des moyens très limités, ne cherchant donc pas uniquement l'épuisement d'un adversaire mais bien sa défaite. La manœuvre aéroterrestre, le transport logistique maritime et aérien deviendront alors de plus en plus risqués. Les réponses conventionnelles à disposition d'un état sont nécessairement plus coûteuses qu'elles passent par la dispersion, la protection des forces, la dissuasion ou la rétorsion.

Les lanceurs de précision mobiles exigeront la mise en place de systèmes défensifs plus élaborés, de systèmes d'alerte, de localisation, voire de neutralisation modernes pour limiter ce type de menaces, sans réellement pouvoir en venir à bout. Pour autant, les temps de réponse des systèmes de détection et d'interception ne permettent pas une protection suffisante face aux armements d'infanterie. Les moyens de contrer ces menaces sont inexistantes ou inadaptés. Le brouillage GPS peut offrir une relative parade contre des armements guidés GPS, mais au risque de perturber les systèmes amis ou de ne pas maîtriser les zones d'impact des projectiles brouillés.

Il convient donc, pour assurer une protection suffisante aux forces déployées, de privilégier des zones de déploiement pérennes qu'il sera possible de rendre résilientes aux attaques potentielles. Cette protection passe dans un premier temps par l'établissement

de périmètres sécurisés suffisants pour empêcher les tirs directs et les actions commando ou suicides. Le durcissement des infrastructures projetées doit ensuite être envisagé afin qu'elles soient en mesure de résister à des tirs d'armements d'infanterie et qu'elles permettent le travail en environnement hostile et dégradé. L'enterrement des infrastructures les plus sensibles, tels les postes de commandement ou les dépôts d'armement, doit être étudié pour supporter les attaques les plus conséquentes. Enfin, le camouflage des sites doit être systématique, pour empêcher l'identification et la géolocalisation des zones vulnérables et contrer les capacités de ciblage de précision.

On comprend ainsi que les surcoûts associés à ces mesures de protection sont difficilement compatibles avec l'établissement de bases précaires dans un temps contraint. Il semble donc judicieux de privilégier l'accès pérenne à des bases projetées durcies dans des emplacements stratégiques tels que Niamey, Djibouti, H5 (ou Base aérienne Prince-Hassan) en Jordanie ou encore Al-Dhafra aux Émirats arabes unis. L'action diplomatique, les coopérations stratégiques et les relations profondes entre la France et ces pays d'importance stratégique doivent ainsi être menés avec volontarisme pour y garantir notre accès et celui de nos alliés principaux.

Développer des capacités d'entrée en premier adaptées

Aspects capacitaires

À un horizon de dix ans et compte tenu du temps nécessaire à la mise en œuvre opérationnelle de nouveaux systèmes d'armes complexes permettant de garantir la supériorité technologique, seuls le développement d'équipements simples et peu coûteux ou l'achat sur « étagère » peuvent contribuer à réduire les effets de stratégies de déni de zone. L'intérêt de ces systèmes d'armes ou équipements réside dans leur capacité à interconnecter les systèmes existants, à maîtriser le spectre électromagnétique et à saturer les défenses adverses.

Les systèmes d'armes doivent avant tout coopérer pour augmenter leur efficacité opérationnelle dans un environnement non permissif. Pour cela, il devient fondamental de chercher à les interconnecter afin de partager l'information en temps réel et ainsi d'améliorer l'autoprotection et la connaissance du champ de bataille pour l'ensemble des forces engagées. Cette collaboration est aujourd'hui rendue possible par la mise en réseau des plateformes, qui autorise une plus grande flexibilité dans leur positionnement et la combinaison des effets. Le combat collaboratif et la fusion de l'information offrent au commandement la possibilité de géolocaliser ses forces, de développer une meilleure compréhension de l'environnement, et ainsi de permettre des décisions plus rapides.

Le partage de l'information est par exemple l'objectif du programme *Scorpion*, lancé par l'Armée de terre en 2014. Au cœur de ce programme majeur, *Contact* est un élément essentiel qui vise notamment à tirer parti des possibilités de combat collaboratif au travers du concept d'infovalorisation ⁽¹³⁾ et de numérisation du champ de

(13) Démultiplication des effets opérationnels d'une plateforme par sa mise en réseau avec d'autres plateformes.

bataille. Il importe de veiller à la généralisation du combat collaboratif par une véritable interopérabilité des équipements et des systèmes d'interconnexion dans les trois armées, soit par la généralisation du programme *Contact*, soit en privilégiant les initiatives technologiques qui rendent compatibles les différents équipements des armées.

Face à des stratégies de déni de zone, l'aptitude à réduire la capacité de l'adversaire à engager des cibles passe par le leurrage ou la saturation de ses systèmes de détection. La maîtrise du spectre électromagnétique, notamment dans la phase d'entrée en premier, est essentielle pour introduire de l'incertitude et de la confusion dans les défenses intégrées et les systèmes de ciblage d'un adversaire utilisant des moyens modernes. Elle peut par exemple permettre une pénétration partiellement masquée des défenses adverses, la perturbation du fonctionnement des outils d'aide à la décision et le ralentissement de la boucle décisionnelle. La création dans le spectre électromagnétique, voire dans le domaine cybernétique, de situations virtuelles noyant des plateformes réelles, réduit le niveau de risque sur les forces engagées et leur permet de mener leur mission avec de meilleures chances de survie.

De même, la saturation des défenses par des plateformes physiques multiples contribue à une meilleure protection des forces. Pour exemple, le *Miniature Air Launched Decoy* (MALD ou Leurre aérien miniature) développé pour les forces armées américaines dans le but de saturer les défenses. Mobile aérien léger (150 g) à bas coût délivré par un aéronef pour multiplier les échos radar, il permet de noyer les plateformes opérationnelles dans un environnement aérien suffisamment dense pour réduire l'efficacité des défenses aériennes adverses. D'une portée de près de 1 000 km, ce leurre intelligent réalise des trajectoires préprogrammées après son lancement et imite la signature et les comportements des aéronefs engagés pendant 20 à 45 minutes dans la zone d'opération. Une version capable de réaliser du brouillage électromagnétique individuel ou coopératif a également été développée⁽¹⁴⁾. D'un coût unitaire variant de 30 000 à 120 000 dollars, ce système pourrait aisément être acheté sur étagère et adapté aux moyens nationaux pour augmenter notablement leur capacité de pénétration dans une phase d'entrée en premier.

À plus long terme, d'autres solutions capacitaires plus onéreuses existent pour maintenir une avance technologique garantissant ces capacités d'entrer en premier. L'aptitude à tirer de plus loin, avec des armements « hypervéloces » et des plateformes disposant d'une plus grande furtivité sont des pistes qu'il s'agira de développer à un horizon 15-20 ans afin de conserver l'avantage technologique par rapport à nos adversaires.

Redécouvrir la manœuvre

Au-delà de ces aspects capacitaires, la réussite d'un engagement exige en fait la réalisation d'une chaîne complexe d'événements, dont chaque maillon est vulnérable et peut être rompu. Tout en poursuivant les efforts pour maintenir dans le long terme

(14) RAYTHEON : « Mald Decoy: Disrupting Enemy Air Defense Systems » (www.raytheon.com/capabilities/products/mald/).

une supériorité technologique suffisante, il importe donc de veiller à une plus forte synergie des moyens existants ainsi qu'à l'exploitation des failles des concepts adverses pour garantir notre liberté d'action.

Pour cela, la France doit également conserver son avantage organisationnel et doctrinal. L'entretien d'une connaissance fine et actualisée des milieux physiques et humains, la préparation opérationnelle développant aguerrissement, rusticité, force morale, aptitude à la prise de risques calculés tiennent ainsi un rôle majeur afin de tenter de maintenir l'avantage qualitatif dont bénéficient les armées françaises en opérations.

Développer la pensée stratégique et l'anticipation au travers du *wargaming* est également un domaine d'effort qui permettrait de redécouvrir la manœuvre. Les *wargames*, largement pratiqués chez nos alliés anglo-saxons ainsi que dans le monde économique, permettent de simuler une grande variété de scénarios, du niveau stratégique au niveau tactique. Ces simulations, qui ne s'appuient pas nécessairement sur une aide informatique, visent à comprendre les possibles évolutions d'un environnement de conflit afin de présenter des options et de déterminer les options les plus robustes ou les plus adaptées pour y faire face.

Le *wargaming*, qui devrait impliquer les plus hautes autorités militaires, voire les autorités politiques pour le niveau stratégique, vise à penser en dehors des contextes existants et à identifier les failles possibles de notre outil de défense et ses conséquences sur la pérennité de la souveraineté nationale. Il permet également, dans un cadre multinational, d'accroître la coopération avec nos partenaires stratégiques, de développer une compréhension commune des challenges de sécurité et d'identifier des initiatives pour renforcer la coopération au-delà de la sphère militaire.

Lutter dans des espaces non permissifs

Dans un environnement non permissif, la menace, complexe et intégrée, peut être globale ou locale, permanente ou volatile. Les opérations doivent être conduites à proximité ou directement exposés aux menaces dans les trois milieux, engendrant un niveau de risque variable, susceptible de provoquer des pertes et de ralentir la stratégie retenue. Lutter dans des espaces non permissifs sans atteindre une totale liberté de mouvement par la supériorité technologique impose donc une plus grande synergie interarmées tout en étant conscient des risques pesant sur nos forces.

L'acceptation du risque et ses conséquences

La projection de forces et de puissance ne peut évidemment s'envisager que dans la perspective d'une victoire potentielle. L'absence de supériorité dans un engagement, qui induit un risque plus important de pertes, a deux conséquences majeures. D'une part cet engagement n'est concevable pour une Nation que si ses intérêts vitaux sont en jeu : l'action doit être acceptée et assumée par le peuple. Ceci implique que la décision d'engager des forces dans un conflit soit soigneusement pesée, au regard des risques à court et long termes comme vis-à-vis des gains attendus.

D'autre part, accepter des pertes dans un engagement impose de disposer de réserves suffisantes pour durer. Les moyens dont dispose la Nation doivent ainsi être progressivement dimensionnés, tant en nombre de systèmes d'armes disponibles que de personnels pour être en mesure d'absorber une attrition tant humaine que matérielle.

Opérer dans un espace non permissif ou contesté

Mener d'une façon durable des opérations de combat sans détenir une totale liberté de mouvement, faute de supériorité technologique, impose d'obtenir l'ascendant par d'autres moyens. Il reste pour autant indispensable d'obtenir un certain niveau de supériorité aérienne, même s'il n'est atteint que localement et temporairement. Dans le cas contraire, le *Field Marshal* Bernard L. Montgomery soulignait : « *If we lose the war in the air, we lose the whole war and lose it quickly* »⁽¹⁵⁾. Face aux défenses modernes, seule une meilleure synergie interarmées permettra d'atteindre une gestion multi-tâches plus efficace des différentes activités qui contribuent à une opération, dans le but de raccourcir les cycles décisionnels et ainsi de reprendre l'ascendant sur l'adversaire.

Cette synergie doit être le fruit d'une évaluation de la situation partagée par la mise en réseau de l'ensemble des acteurs tactiques et opérationnels, d'une adaptabilité et d'une flexibilité renforcée par une vision opérationnelle commune de la situation et l'accès à une variété accrue des modes d'action. Elle s'exprime avant tout en variant les options de déploiement sur zone et en protégeant les capacités spatiales et cybernétiques tout en attaquant celles de l'adversaire. En manœuvrant initialement depuis des distances stratégiques, cette synergie doit permettre d'exploiter la supériorité des forces dans un domaine donné pour contourner les capacités adverses de déni d'accès s'exerçant dans un autre domaine. La saturation des systèmes de l'adversaire est ainsi obtenue en menant des actions simultanées sur plusieurs fronts d'opérations, en exploitant au mieux la surprise et la déception et en attaquant les capacités adverses dans la profondeur.

Un tel niveau de coopération ne s'obtiendra qu'au prix d'un nouvel effort en matière d'intégration interarmées, tant au niveau organisationnel – formation, entraînement, culture – que capacitaire – vision globale des effets à obtenir.

**

Ainsi, des stratégies d'alliance ciblées et une protection crédible de nos forces projetées peuvent maintenir durablement l'accès stratégique aux zones d'opérations. Des ajustements capacitaires mineurs et l'optimisation de la manœuvre doivent permettre de garantir l'entrée en premier. Enfin, l'acceptation d'un niveau de risque supérieur, indissociable d'un engagement légitime ainsi qu'une meilleure synergie interarmées sont les gages du maintien de notre capacité à opérer dans des milieux non-permissifs.

(15) Citation largement diffusée, mais non contextualisée.

Conclusion

Les menaces qui compliquent nos capacités expéditionnaires ne nous imposent pas pour autant une attitude isolationniste dans les années à venir. La volonté de la France de rester un acteur majeur pour la stabilité internationale et ses intérêts globaux – économiques et militaires – sont autant de raisons pour ne pas nous rétracter sur nous-même. Mais les risques nouveaux que font peser la prolifération de systèmes d'armes performants et les stratégies de déni d'accès sur nos modes d'actions, qui réduisent une supériorité technologique de plusieurs décennies, imposent de mesurer nos actions futures à l'aune de nos intérêts stratégiques et de l'acceptation d'un niveau d'attrition supérieur.

Pour réduire ces risques, une nouvelle étape dans l'interarmisation doit être franchie en matière organisationnelle, doctrinale et programmatique. Mais il importe aussi de savoir quelle réponse la France sera prête à apporter aux crises futures, selon quel niveau d'ambition et selon quels objectifs. C'est bien cette ambition, cette volonté politique, qui permettra d'assumer les risques et de conserver notre capacité d'action.

Éléments de bibliographie

BRUSTLEIN Corentin, « L'entrée en premier et l'avenir de l'autonomie stratégique », *Focus Stratégique* n° 70, Ifri, novembre 2016 (www.ifri.org/sites/default/files/atoms/files/entree_en_premier_brustlein_2016.pdf).

BRUSTLEIN Corentin, « Vers la fin de la projection de force », *Focus Stratégique* n° 20, Ifri, avril 2010 (www.ifri.org/sites/default/files/atoms/files/fs20brustlein_2.pdf).

DoD, *Joint Operational Access Concept (JOAC)*, version 1.0, 17 janvier 2012 (www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf).

GILLET Benjamin, « Le concept de *Multi-Domain Battle* : l'illustration du pouvoir normatif de la recherche militaire américaine », *La Note du CESA* n° 105, janvier 2017.

GROS Philippe, « La question du déni d'accès et le concept Air-Sea Battle », *Note de la FRS*, n° 17, 18 juin 2013 (www.frstrategie.org/publications/notes/la-question-du-deni-d-acces-et-le-concept-air-sea-battle-17-2013).

RAMEL Frédéric, « Accès aux espaces communs et grandes stratégies : vers un nouveau jeu mondial », *Études de l'Irsem* n° 30, 2014 (www.defense.gouv.fr/irsem/page-d-accueil/vient-de-paraitre/etude-de-l-irsem-n-30-2014).

RICHARDSON John (Chief of Naval Operations, Adm.), « Deconstructing A2AD », *The National Interest*, 3 octobre 2016 (<http://nationalinterest.org/>).

« Otan : faire face au déni d'accès », TTU, 14 mars 2016 (www.ttu.fr/otan-faire-face-deni-d-accses/).

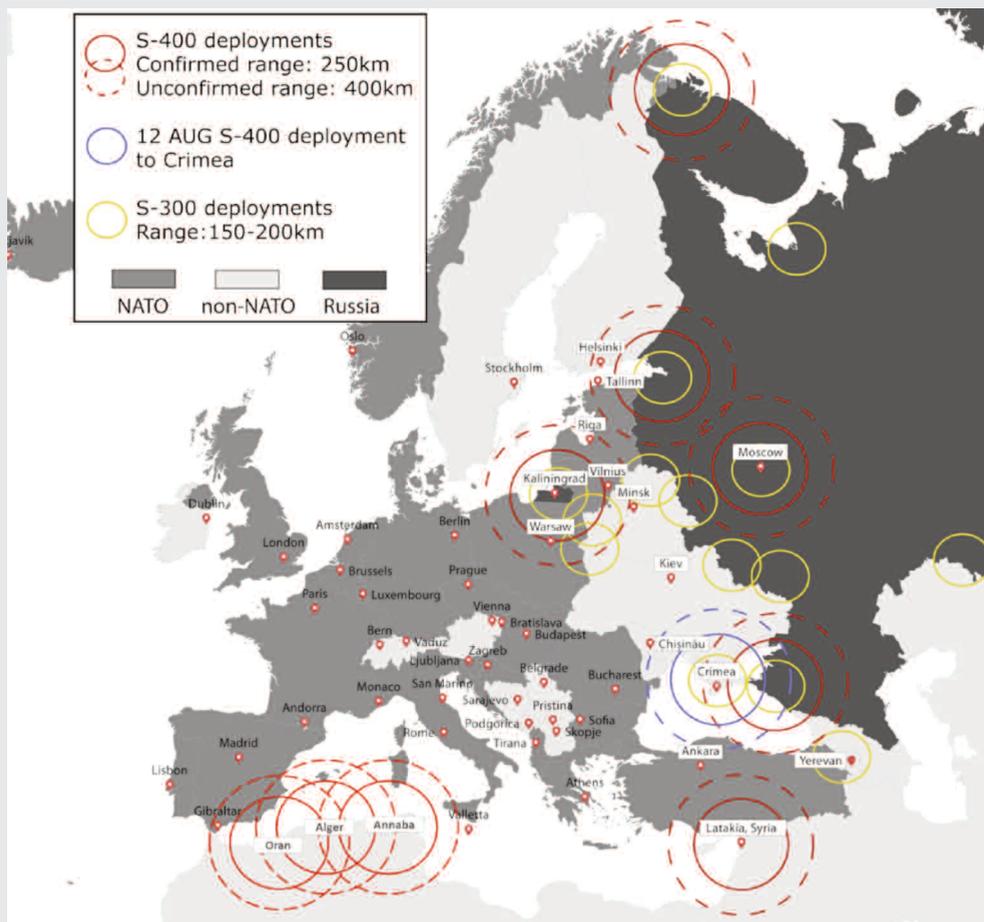
MALDERA Nicolas, « La mutation technologique de l'Armée de terre, le cas du programme *Scorpion* », Ifrap, 20 juin 2016 (www.ifrap.org/).

Entretiens

- Général de brigade aérienne Bruno PACCAGNINI, Chef du bureau « Prospective et stratégie militaire » de l'État-major des armées (EMA).
- Capitaine de vaisseau François MOREAU, Officier de cohérence d'armée à l'État-major de la Marine.
- Ingénieur général de l'armement Lionel MORIN, Directeur du Centre d'analyse technico-opérationnelle de Défense.
- Alexis BOISARD, Centre d'analyse technico-opérationnelle de Défense.
- Dr Corentin BRUSTLEIN, chercheur, responsable du Centre des études de sécurité de l'Ifri (Institut français des relations internationales) et du programme « Dissuasion et prolifération ».

Quelles orientations face au déni d'accès à l'horizon 2025 ?

ANNEXE I - LA PROLIFÉRATION DES MOYENS DE DÉNI D'ACCÈS STRATÉGIQUE ⁽¹⁶⁾



L'Algérie possède, depuis 2003, plusieurs régiments équipés de systèmes de missiles sol-air russes *S-300* qui protègent le nord du pays, le littoral, ainsi que ses frontières avec le Maroc. Selon diverses sources *Internet* ⁽¹⁷⁾, elle pourrait être un des premiers acheteurs étrangers des missiles russes *S-400*, ce qui consoliderait sa défense aérienne en lui permettant d'engager des cibles jusqu'au Nord de la Tunisie. Ces systèmes, parfaitement intégrés au sein du Commandement des forces de défense aérienne du territoire, garantissent la protection de l'espace aérien algérien. Par ailleurs, les forces armées aériennes sont équipées de plusieurs intercepteurs performants de type *Su-35*, *Su-30 MKA*, *Mig-29S* et *Mig-25*. Sur le plan maritime, l'Algérie possède 6 sous-marins de classe *Kilo* qui, outre leur capacité anti-navire, pourraient également être armés de missiles *S-300*. Plusieurs frégates de classe « Koni » et « Meko-200 », ainsi que des corvettes de classe « Nanuchka » et « Djebel », complètent une marine de guerre professionnelle.

(16) Carte issue de l'*Institute for the Study of War*, août 2016, et modifiée pour intégrer les défenses algériennes (en version couleur dans l'édition numérique de ce cahier, en noir et blanc dans la version papier).

(17) Notamment sur la page *Wikipedia* de l'Armée algérienne ([https://fr.m.wikipedia.org/wiki/Armée_nationale_populaire_\(Algérie\)](https://fr.m.wikipedia.org/wiki/Armée_nationale_populaire_(Algérie))).

Quelles orientations face au déni d'accès à l'horizon 2025 ?

ANNEXE II - LES *G-RAMM* (*GUIDED ROCKET, AMMUNITION, MORTAR, MISSILES*)

Historiquement, l'impact stratégique des roquettes a été établi durant la deuxième guerre mondiale avec les *V1* et *V2*, et plus récemment avec les missiles *SCUD*. En 2005, l'*USS Ashland*⁽¹⁸⁾ avait été la cible de missiles *Katyushas*, ce qui provoqua son appareillage immédiat depuis le port où il faisait escale en Jordanie. Des milliers de roquettes *Katyusha/Kassam* ont également été tirées lors de la crise au Liban en 2006, générant des représailles aériennes et un profond malaise en Israël. Selon le Département de la Défense américain (*DoD*), la probabilité de prolifération de ces systèmes est particulièrement élevée d'ici 2020.

Le développement des systèmes d'artillerie guidée a quant à lui débuté en 1980 avec le *M712 Copperhead* (États-Unis). Délivrant des obus guidés laser de 155 mm, ce système était destiné à détruire principalement des chars, mais n'a jamais connu un réel succès en raison d'un manque de fiabilité et de difficultés à coordonner l'éclairage laser de la cible. Pour autant, la Russie a rapidement mis en œuvre son propre système d'artillerie au milieu des années 1980, le *Krasnopol 152/155*. Exporté en Chine, en Inde, au Belarus, en Ukraine et au Venezuela, ce système était supérieur au *Copperhead* en termes de portée notamment. La France a développé pour sa part l'obus *Bonus*, en service dans les forces.

Les systèmes américains actuellement en service tel que l'*Excalibur* sont aujourd'hui guidés par *GPS*. Ces systèmes, ou leurs équivalents russes ou chinois, représentent un danger important en termes de prolifération.

Concernant les mortiers, plusieurs pays ont poursuivi le développement de systèmes guidés (le *Merlin* britannique, l'*Aquila* français, le *Strix* suédois, le *Fireball* israélien, le *Grand/Smel'chak* russe). Ces obus de mortier guidés par infrarouge, laser ou bien radar sont réellement attractifs pour les groupes terroristes en particulier. Leur létalité, leur simplicité d'emploi en font des armes redoutables à courte distance. Ils constituent ainsi une des principales menaces à court terme pour les troupes déployées dans des conflits de type contre-insurgence, d'autant plus que leur coût est amené à baisser avec leur prolifération.

Enfin, une grande variété de missiles guidés envahit déjà les zones d'opération. Les plus courants sont les missiles courte portée communément appelés *MANPADs*⁽¹⁹⁾ (*SA-18, Stinger...*). Mais de nombreuses autres variantes comment également à proliférer et visent non plus uniquement des aéronefs, mais également des véhicules (*AT-5* et *AT-14* russes), des navires (*C-802*, utilisé par le *Hezbollah*) et des troupes. Enfin, certains acteurs seront bientôt en mesure de délivrer ces missiles à l'aide de drones bon marché proliférant.

ANNEXE III - DÉPENSES MILITAIRES DANS LE MONDE⁽²⁰⁾

Après des décennies de baisse ou de stagnation, la tendance s'inverse à partir de 2015 avec des dépenses mondiales d'armement estimées par le *SIPRI* (Institut international de recherche sur la paix de Stockholm) à 1 676 milliards de dollars, soit 2,3 % du PIB mondial. Cette hausse recouvre des réalités contrastées, puisque, après des années de hausses frénétiques, certains exportateurs de pétrole comme la Russie ou l'Arabie saoudite ont dû se résoudre à une baisse en 2016.

Seuls quatre pays européens (dont le Royaume-Uni, au 3^e rang des dépenses mondiales avec 53,8 Mds \$, en hausse de 0,5 % en 2016) sur les 28 États-membres de l'Union respectent l'objectif fixé par l'Otan de 2 % du PIB consacré à la défense. Les pays Baltes et de l'Est affichent tous une volonté nouvelle d'investissement, notamment sous la pression de la Russie.

Le surplus de commandes d'armes dans le Golfe est justifié par l'instabilité liée au terrorisme islamique et à la compétition qui se joue entre l'Arabie saoudite et l'Iran. L'Asie dépense déjà 100 Mds \$ de plus pour sa défense que tous les Européens, sous l'impulsion d'une Chine de plus en plus offensive qui incite à la prolifération. Longtemps cantonnée dans une attitude défensive, Pékin a augmenté ses dépenses militaires de 132 % au cours des dix dernières années. Elle possède le 2^e budget militaire mondial (191 Mds, en hausse de 5 %). Longtemps dépourvue de capacité de projection, la Chine se dote à toute vitesse d'une flotte militaire de premier rang, qui fait peser le risque d'une prolifération massive d'équipements de haute technologie à bas coût. L'Inde vient de voter un budget militaire en hausse de 8 %. Elle a gagné deux places en 2016 au palmarès des dépenses, au 4^e rang désormais, et pourrait également être une source de prolifération.

ANNEXE IV - LES DIFFÉRENTS NIVEAUX DU DÉNI D'ACCÈS STRATÉGIQUE

Sur le bas du spectre des menaces, les *G-RAMM*, pour la plupart déjà en service, menacent bien plus sérieusement les forces déployées qu'auparavant compte tenu de la précision de leur guidage.

Au niveau intermédiaire, une multitude d'armements et de modes d'action peuvent présenter un risque pour les forces déployées à distance. Les événements du 1er octobre 2016 au Moyen-Orient illustrent parfaitement cette menace sur les espaces communs.

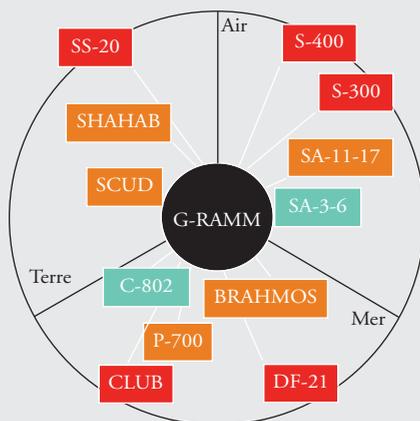
Dans le haut du spectre, les domaines maritimes et aériens sont particulièrement menacés par la prolifération de systèmes d'armes russes ou chinois de plus en plus performants et accessibles.

(18) Navire TCD de classe « Whidbey Island » de l'*US Navy*.

(19) *Man Portable Air Defense Systems*.

(20) Anne BAUER, « Les dépenses militaires augmentent partout dans le monde, et d'abord en Asie », *Les Échos*, 10 janvier 2017 (www.lesechos.fr/).

Quelles orientations face au déni d'accès à l'horizon 2025 ?



Exemples d'armements défensifs dans les milieux terrestres, maritimes et aériens, selon leur portée

ANNEXE V - LES CONCEPTS AMÉRICAINS

Le concept d'Air-Sea Battle (ASB)

Les États-Unis ont lancé dès 2008, sous l'égide de l'*US Air Force (USAF)* et de l'*US Navy*, des réflexions conceptuelles motivées par la montée en puissance des capacités *A2AD* de la Chine. Le concept d'*ASB* repose ainsi sur l'amélioration de l'efficacité mutuelle des moyens engagés et une coopération plus étroite entre les forces armées. L'interconnexion des domaines aérien et maritime aggrave plus encore la dépendance en matière de projection de forces. La perte potentielle de sanctuaires traditionnels et la dilution des domaines exigeaient que l'*USAF* et l'*US Navy* établissent une relation plus coopérative. Le concept d'*ASB* proposait que cette relation fonctionne sur trois niveaux distincts mais liés : l'intégration, la formation et les équipements.

Au niveau institutionnel, il s'agissait d'engendrer un niveau de confiance suffisant pour ériger le cadre de la future coopération entre les services. La création d'un « *ASB Integration Office* » a été un effort institutionnel conjoint qui avait pour but de favoriser une meilleure coopération tout en permettant de maintenir une dynamique bénéfique au processus de montée en puissance du concept.

Au niveau opérationnel, l'objectif était d'organiser et d'entraîner les forces ensemble au sein des commandements les plus concernés. L'*ASB* avait ainsi pour but de conduire à un effort renouvelé pour former les équipages de l'*USAF* à réaliser des missions traditionnellement dévolues à la *Navy* comme la lutte antisurface, ou pour former des équipages de frégates *Aegis* à la mission de protection des bases aériennes.

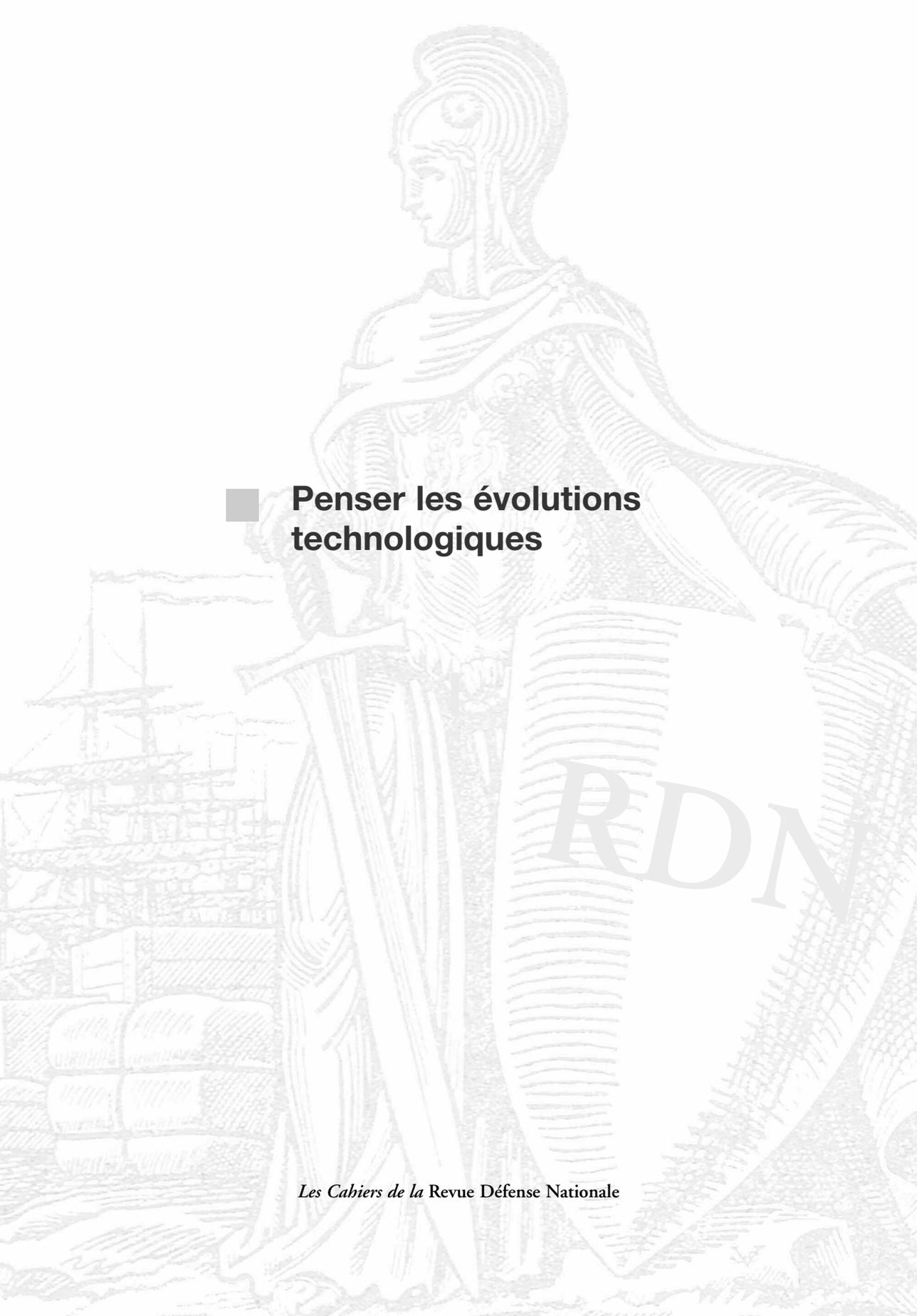
Au niveau des équipements, l'effort était porté sur un niveau d'intégration et d'interopérabilité élevé des équipements. L'*USAF* et l'*US Navy* s'efforcent ainsi d'utiliser leurs systèmes d'armes de façon innovante pour accomplir des missions traditionnellement dévolues à un service. Équiper les sous-marins des moyens de réception et de traitement en temps réel des flux d'informations fournis par l'*USAF* afin d'alimenter leurs missiles de croisière en données actualisées (avant et après le tir) est une voie de coopération.

L'évolution vers le JOAC

Controversé compte tenu d'une initiative insuffisamment interarmées et d'une focalisation sur le déni d'accès stratégique plus que sur l'interdiction de zone, le concept d'*ASB* a laissé la place à partir de 2012 au *Joint Operational Access Concept (JOAC)* qui structure la *Joint Access and Maneuver in Global Commons (JAM-GC)* élaborée en 2015. Ces nouveaux concepts visent à contrer les capacités de déni d'accès en perturbant les systèmes adverses par une synergie interdomaines renforcée dans un tempo supérieur ⁽²²⁾.

(21) Alors qu'un navire de transport logistique émirien *HSV-2 Swift* était sur le point de traverser le détroit de Bab-El-Mandeb, plusieurs missiles antinavires chinois *C-801* l'endommagent gravement dans le but d'étrangler les mouvements des navires de guerre des Émirats arabes unis dans la région. Quelques jours plus tard, ce sont les navires américains qui sont visés par des tirs de missiles *C-802*, et la ville saoudienne de Taïf par des missiles *SCUD-D* à 700 km de la frontière yéménite. Par ces actions indirectes, l'Iran montre ainsi la fragilité de l'accès aux espaces communs et la vulnérabilité de nos moyens de projection de forces.

(22) Philippe GROS, « La question du déni d'accès et le concept *Air-Sea Battle* », *Note de la FRS* n° 17, 18 juin 2013.



■ **Penser les évolutions
technologiques**

RDN

Robots et intelligence artificielle : quelle place pour l'homme dans les futures capacités militaires françaises ?

Olivier BEAURENAUT

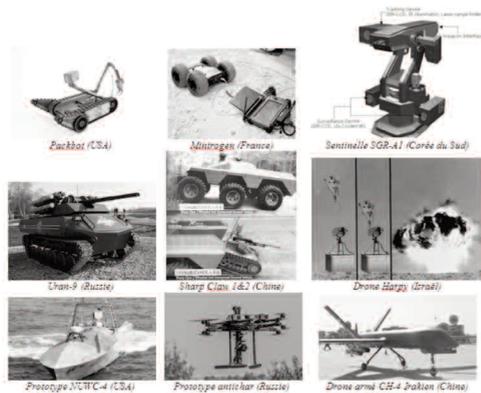
Ingénieur en chef de l'armement, auditeur de la 66^e session
du CHEM.

Si chaque outil pouvait recevoir nos ordres, ou les anticiper pour exécuter chacune des tâches qui lui seraient assignées [...], et si de la même manière les navettes tissaient automatiquement, si les plectres jouaient tout seuls de cithare, alors les constructeurs n'auraient plus besoin d'assistants, et les maîtres n'auraient plus besoin de serveurs.

Aristote (384 à 322 avant J. C.), *Politique* 1.2.4-5

La robotique correspond à la convergence de plusieurs domaines technologiques qui ne sont pas nouveaux : mécanique, électronique et télécommunications, technologies de l'information et intelligence artificielle. Née dans les années 1950, cette dernière a d'abord vu son développement contrarié par des puissances de calcul limitées malgré une croissance exponentielle suivant la loi de Moore. Ce n'est qu'à partir des années 1990 que les premiers systèmes intégrant une intelligence artificielle sont apparus au sein de systèmes experts, mono tâche dans un premier temps. Les puissances disponibles et la miniaturisation des composants permettent aujourd'hui, pour un coût modique, d'intégrer des logiciels capables d'accomplir de plus en plus de tâches qui, jusqu'à présent, n'étaient réalisables que par l'homme.

Cette note vise à fournir un éclairage, le plus objectif possible, sur les enjeux, les débats, les opportunités et les risques liés à la robotisation des capacités militaires ; elle propose des actions pouvant contribuer à la définition et la mise en œuvre d'une stratégie robotique globale de défense. La description des technologies et de leurs développements a été volontairement exclue, afin de rester accessible à un public non scientifique. La perspective sur l'intelligence artificielle a été limitée à une quinzaine d'années, pour ne pas entrer dans les débats trans-humanistes



Exemples de robots en service ou en développement

sur des intelligences artificielles supérieures à l'homme ⁽¹⁾, dont l'apparition est prédite au-delà de 2030.

Parmi les nombreuses définitions disponibles, le terme robot employé ci-après correspond à une machine disposant à la fois de moyens de perception de l'environnement (senseurs), de capacités de traitement de l'information (de calculs voire cognitives) et de moyens d'action sur son environnement. Cette définition a l'intérêt de ne pas fermer la question de la place de l'homme et de l'autonomie, ni de se limiter aux robots « physiques » : en effet, nous verrons plus loin que les questions attachées aux robots intervenant dans le champ informationnel ou immatériel présentent une criticité importante pour le domaine militaire.

La 4^e révolution industrielle est en marche

Transformation importante et rapide du secteur civil

Le développement des véhicules autonomes, technologie dans laquelle s'engouffrent non seulement tous les constructeurs automobiles, traditionnels (Ford, BMW, PSA...) ou nouveaux entrants (Google, Tesla...), vient en premier à l'esprit quand il s'agit d'illustrer l'irruption de l'intelligence artificielle et de la robotique dans les activités humaines. Cette transformation, souvent qualifiée de « quatrième révolution industrielle », sera bien plus profonde que ses manifestations les plus médiatiques. Elle progresse déjà actuellement dans tous les secteurs de l'économie, y compris les plus inattendus comme en atteste par exemple l'adoption du robot Ross d'IBM dans les cabinets d'avocats ou dans le domaine de l'assurance.

De multiples études parues ces derniers mois mettent en évidence l'impact majeur prévisible sur les activités humaines : la numérisation pourrait concerner à terme plus d'un tiers des emplois des pays de l'Organisation de coopération et de développement économiques (OCDE), et, d'ici 2020, nécessiter la reconversion de 7 millions d'emplois dans les pays développés.

Les précédentes révolutions industrielles (mécanisation ou communications par exemple) avaient profondément modifié le monde militaire. Il ne fait pas de doute qu'une fois encore, celui-ci se verra profondément impacté par ces transformations.

Malgré une longue histoire, des perspectives actuellement limitées dans le domaine militaire

Les premiers systèmes d'armes robotisés sont apparus il y a tout juste un siècle avec des prototypes d'engins télécommandés aériens, de surface ou terrestres testés à la fin de la Première Guerre mondiale. Le secteur aérospatial a vu se poursuivre le mouvement au milieu du XX^e siècle, avec le développement des engins cibles issus notamment des technologies de missiles *VI* et *V2* (en France le *CT 10* à partir de 1946).

(1) Ceux-ci faisant l'hypothèse qu'un point de singularité sera atteint, déclenchant un emballement de la croissance technologique, dès qu'une machine pourra s'auto-améliorer et de créer de nouvelles générations artificielles.

Robots et intelligence artificielle : quelle place pour l'homme dans les futures capacités militaires françaises ?

Ce n'est réellement qu'à partir de l'engagement israélien au Liban en 1982 que les drones ont commencé à trouver leur place dans les capacités militaires, en participant pleinement à la manœuvre aérienne dans la plaine de la Bekaa : utilisés pour la reconnaissance et le renseignement électronique, mais également pour stimuler les défenses, provoquer des tirs de missiles antiaériens syriens permettant aux chasseurs à capacités antiradar de riposter.

Les robots sont aujourd'hui devenus incontournables pour certaines capacités en opérations ; leur nombre et la fréquence de leur utilisation croissent rapidement dans l'ensemble des armées occidentales ⁽²⁾. Ainsi, pour lutter contre les engins explosifs improvisés (*IED*), la France a déployé en 2012 le robot *Minirogen* en Afghanistan. Dans la Bande sahélo-saharienne (BSS), elle emploie ses drones *Reaper* au maximum des capacités des vecteurs et des équipages : le cap des 15 000 heures de vol cumulées a été franchi début 2016 (2 400 h seulement en 2014). De manière moins visible, la Marine nationale utilise depuis plusieurs années des engins robotisés pour la détection de mines sous-marines.

Au-delà de ces « robots physiques », des « robots informatiques » sont déjà opérationnels dans les forces. Les frégates françaises *Horizon* disposent d'un mode d'engagement totalement automatique pour l'autoprotection antimissile, à l'instar du système *Phalanx* américain. Plus récemment, les logiciels de *data mining* se sont imposés dans le domaine du renseignement.

Malgré cette accélération récente, les perspectives à 15 ans de la robotique sur les grands programmes d'armement apparaissent encore assez limitées, sans comparaison avec l'explosion en cours dans le secteur civil. Dans le domaine terrestre, une robotisation significative ne semble accessible qu'au-delà de 2025 dans de futures étapes du programme *Scorpion*. Dans le domaine aérien, les travaux de conception d'un prototype d'aéronef de combat non habité débutent à peine (projet *FCAS – Future Combat Air System* – franco-britannique). Enfin, si les avancées sont réelles pour le naval avec le lancement en 2016 du programme de guerre des mines futur (programme *SLAMF – Système de lutte anti-mines futur* – qui intégrera plusieurs systèmes robotisés de surface et sous-marins dont un prototype est en cours de réalisation en coopération franco-britannique), les *Frégates de taille intermédiaire (FTI)* constitueraient *a contrario* une régression du point de vue de l'automatisation, tout en répondant à un besoin de soutenabilité sur le plan des ressources humaines (équipage probablement plus nombreux que celui des *Frégates multimissions* ou *Fremm* conçues à partir du début des années 2000).

D'ici une quinzaine d'années, le paradigme qui prévalait d'excellence technologique des capacités militaires par rapport aux produits de grande consommation pourrait se trouver totalement inversé.

(2) Les Américains déployaient ainsi plus de 12 000 robots terrestres en Irak en 2008 (il n'y en avait aucun en 2003).

Évolution des rapports de force et fin de la suprématie des grandes Nations occidentales

Le développement de la robotique et de l'intelligence artificielle vient remettre fortement en question un des fondements de notre puissance militaire : notre modèle, calqué sur celui des États-Unis, repose notamment sur notre supériorité technologique.

La première raison est le caractère naturellement proliférant des technologies du numérique, qui ne nécessitent pas, pour être implémentées, les savoir-faire spécifiques détenus par une base industrielle de défense, qui sont parfois non « documentables » ou numérisables et dont la transmission passait jusqu'à maintenant essentiellement par le transfert d'expérience ⁽³⁾.

Les logiciels sont par nature proliférants (ils peuvent être transférés aisément et dupliqués à l'infini). En outre, toutes les briques nécessaires pour réaliser des robots autonomes seront accessibles dans le monde civil : en caricaturant à peine, les briques logicielles et les capteurs des voitures autonomes permettront d'appréhender l'environnement, d'assurer la mobilité et de déterminer des itinéraires, y compris en milieu non coopératif ou variable ; les moteurs de jeux vidéo permettront d'élaborer des stratégies victorieuses, ainsi que des modes et lignes d'action face à un adversaire non coopératif comme c'est déjà le cas pour les jeux d'échec ou de go ; les drones du commerce quant à eux permettront de disposer des liaisons de données et traitements vidéo nécessaires pour l'appréciation de la situation, de l'environnement, ainsi que les communications. Ceci sans parler de la facilité à fabriquer les robots par impression 3D, ou à les armer : explosifs, armes, générateurs de signaux pour le brouillage étant aisément accessibles.

La seconde raison mettant à mal l'excellence technologique française est liée à notre capacité à investir suffisamment dans ces technologies pour ne pas se faire très rapidement distancer : le budget fédéral américain a consacré en 2014 près de 400 M\$ aux investissements dans le domaine de l'intelligence artificielle, huit fois plus qu'en 2012 et, parmi les 18 Md\$ qui doivent être consacrés aux nouvelles technologies pour la défense, 3 Md\$ devraient être consacrés au seul sujet de la coopération homme-machine sur les cinq prochaines années. Les États-Unis ne sont pas les seuls à s'engager massivement dans cette transformation. Au niveau mondial, le nombre de publications dans le seul domaine du *deep learning* ⁽⁴⁾ a été multiplié par douze entre 2012 et 2015. Depuis 2014, la Chine a dépassé en volume les États-Unis dans ce domaine : elle publie dorénavant presque dix fois plus que la France et a prévu de consacrer 13 Md€ d'ici 2019 à l'intelligence artificielle ⁽⁵⁾.

(3) On peut par exemple citer le rôle clé des compagnons dans une entreprise telle que Dassault Aviation, au cœur des compétences et du patrimoine immatériel de cette société.

(4) Le *deep learning* est une catégorie particulière des techniques d'auto-apprentissage des machines (*machine learning*) qui consistent à entraîner un algorithme en se basant sur des exemples. Dans le cas du *deep learning*, contrairement aux méthodes de *machine learning* traditionnelles, les caractéristiques essentielles du traitement ne sont plus prédéfinies par l'homme, mais élaborées par l'algorithme lui-même.

(5) La Chine dispose d'industriels crédibles : le moteur Baidu annonçait en 2015 avoir battu Google dans la reconnaissance d'images.

La France pourrait fort bien se trouver avant dix ans en position de forte asymétrie technologique face aux États-Unis et la Chine. Conséquemment, elle pourrait le devenir également face aux pays constituant leurs marchés export. L'accessibilité importante de ces technologies pourrait en outre nous amener en position de symétrie technologique ou de faible avantage face aux organisations non étatiques de type terroriste utilisant des technologies civiles.

Les opportunités de la robotique et l'intelligence artificielle pour l'action militaire

Les robots confrontés aux principes de la guerre et à son évolution

Si jusqu'à présent, l'introduction des robots dans les capacités militaires a été limitée à la seule volonté d'affranchir l'homme de certaines tâches précises liées à des situations répétitives ou dangereuses ⁽⁶⁾, la robotique et l'intelligence artificielle vont en réalité modifier bien plus profondément et globalement notre stratégie, notre modèle d'armée, voire les modalités et les fondements de l'action militaire, de l'usage légitime de la force.

En effet, confrontés aux principes traditionnels de la guerre, l'intelligence artificielle et les robots sont susceptibles de présenter des progrès importants par rapport aux capacités traditionnelles en termes d'économie des moyens (optimisation des dispositifs en qualité et quantité sur la base de nombreuses simulations d'engagement et de désengagements, capacité accrue de renseignement...), de concentration des efforts (réunion des forces et synchronisation des actions, fulgurance des effets *via* le réseau, rapidité de traitement des informations et de conduite de l'action...) et de liberté d'action (mobilité affranchie des capacités physiques humaines...).

Au-delà de ces progrès potentiels qui relèvent de la tactique, c'est bien plus en termes de stratégie que ces technologies démontreront tout leur intérêt et constitueront un *game changer*. Elles ont ainsi été placées au cœur de la stratégie américaine du *Third Offset*, élément majeur de l'initiative d'innovation de défense américaine lancée en 2014 : il s'agit en particulier de contrer les capacités croissantes, russes et chinoises, de déni d'accès et d'interdiction de zone, ainsi que de pouvoir faire face au volume important de forces militaires que la Chine est capable d'opposer. Quant aux robots numériques opérant dans le domaine du cyber, sur les médias numériques et réseaux sociaux, ils offrent de nouvelles possibilités de gagner la guerre, sans engagement cinétique, et sont d'une importance majeure dans les doctrines de guerre hybride.

Confrontés aux évolutions récentes de la guerre et aux leçons stratégiques qui peuvent aujourd'hui être tirées, les robots pourraient également constituer une réponse globale, pour affronter les quatre évolutions majeures des engagements : durcissement, digitalisation, distances, durée (4D).

(6) En anglais, on parle de « 3D » : *Dull, Dirty, Dangerous*.

Le domaine de la robotique n'est pas lié à un milieu : des robots peuvent opérer sur terre, mer et dans les airs. Ils ne sont pas limités par l'hostilité des milieux sous-marins et l'Espace, dans lesquels ils sont déjà présents. Ils se développent naturellement dans l'espace numérique (cyber). La robotique peut ainsi être un outil de mise en œuvre de stratégies globales et polyvalentes, y compris dans le champ des perceptions avec les robots numériques interactifs (*chatbots*).

Les robots semblent en outre à même de compléter des capacités traditionnelles numériquement contraintes par la ressource financière ou humaine, afin de satisfaire le besoin du nombre qui résulte à la fois de la taille inédite depuis la Seconde Guerre mondiale des théâtres d'opérations (exemple de la BSS), du besoin de compenser la diminution du format des armées accéléré depuis l'abandon de la conscription et la fin de la guerre froide. En l'espèce, les robots compenseront la diminution de la densité humaine d'occupation militaire ⁽⁷⁾ et n'ont pas de limite autre que celles de leurs batteries (domaine dans lequel le monde civil apportera sans nul doute des gains de performances majeurs ces prochaines années) pour durer sur le terrain.

Ils permettront de compenser l'aversion croissante au risque de notre société, d'éviter les pertes humaines susceptibles de mettre à mal la résilience de la nation et donc la volonté politique. Les robots pourront constituer la nouvelle « chair à canon » nécessaire pour combattre dans les milieux difficiles et dangereux, face à un adversaire mettant en œuvre des modes d'action d'une violence exacerbée et faisant preuve d'un niveau de détermination maximal allant jusqu'au suicide. Ils offrent vitesse et précision à des niveaux inégalables par l'homme, réduisant par la même occasion le nombre des soldats et pilotes exposés à la mort ou aux blessures de guerre. Ceci est d'autant plus important que le risque augmente dans tous les milieux : les avions de combat voient leur impunité et leur liberté d'action contrariées par les capacités *AZAD* (*Anti-Access - Area Denial*) ; la zone urbaine, particulièrement meurtrière pour le fantassin, (re)devient un lieu d'affrontement habituel des forces terrestres ; les capacités militaires navales de surface et sous-marine se banalisent dans le monde. En sauvant des vies ⁽⁸⁾, les robots seraient ainsi à même de préserver ce qui constituerait la principale vulnérabilité de nos forces, le centre de gravité ami ⁽⁹⁾.

Les avantages des robots militaires sur le soldat

Contrairement à l'homme, les robots n'ont pas faim, n'ont pas peur, n'oublient pas les ordres et ne sont pas influençables par les pertes ou le niveau de danger. Ils ouvrent la voie à un dépassement des limites de l'homme au combat au profit de l'efficacité militaire. En mesure d'agir « à la vitesse de l'électron » et non plus limités

(7) Peter W. SINGER dans *Wired for War* compare la période napoléonienne de concentration d'une armée de milliers d'homme sur un unique champ de bataille à une densité de réduite à deux soldats pour un terrain de football pendant la Seconde Guerre mondiale et jusqu'à un soldat pour 780 terrains de football pendant la guerre d'Irak.

(8) Le général Rick LYNCH aurait déclaré lors d'une conférence prononcée en 2009 devant des industriels de l'armement que « sur les 155 hommes de son unité tués en Irak, la vie de 122 aurait pu être sauvée en utilisant des robots ». Cité par Antonin TISSERON, « Robotique et guerres futures : les armées de terre face aux évolutions technologiques », *Cahiers de l'Irsem* n° 12, 2012.

(9) Selon le général américain Robert H. SCALES : « Dead soldiers are America's most vulnerable venter » dans « Urban Warfare: A Soldier's View », *Military Review*, février 2005.

Robots et intelligence artificielle : quelle place pour l'homme dans les futures capacités militaires françaises ?

par nos capacités cognitives, ils s'imposeront dès lors que l'accélération du tempo ne laissera plus de place à l'homme. Dans un monde de plus en plus numérisé et connecté, ils sont seuls à même de mobiliser et d'accéder rapidement aux données de masse. Ils pourraient permettre enfin de mettre en œuvre des capacités tactiques « inhumaines », telle que la modification de forme ou d'échelle ⁽¹⁰⁾.

En termes d'entraînement, l'apprentissage d'un robot est naturellement en progression continue (par enrichissement d'une expérience digitalisée) et quasi instantané (par mise à jour logicielle), alors que la transmission de l'expérience, imparfaite, est à recommencer à chaque génération de soldat ou d'officier et nécessite des durées importantes de formation.

Les robots comme opportunité pour maintenir un modèle d'armée dans un budget contraint

Comment, dans la durée, maintenir des capacités de haut niveau en conservant un niveau de dépenses de défense acceptable, alors que le coût des systèmes d'armes, à quelques exceptions près, bondit à chaque nouvelle génération ?

Pour Peter Warren Singer, spécialiste américain de la guerre moderne, le coût de déploiement d'un soldat (1 M\$ par an entraînement compris) était en Afghanistan considérablement plus élevé que celui d'un robot. L'introduction de robots aura un effet à la baisse sur les dépenses budgétaires liées à l'homme ou à son activité, en volume mais également par recours accru à la simulation pour l'entraînement. Or, l'ensemble constitué par la masse salariale, l'activité opérationnelle et l'entretien programmé des matériels représente une part significative de notre budget de la défense (environ 40 %). L'effet sur les pensions (de l'ordre de 10 Md€ par an) est également à prendre en compte dans cette équation.

Sur les dépenses d'équipements de défense, des effets positifs sont possibles par simplification et allègement des systèmes par rapport aux plateformes habitées (gain de charge utile mais également d'équipements d'accueil des servants et équipages). En outre, la réutilisation de technologies développées par le secteur civil permettra de limiter l'effort de R&D à leur seule adaptation aux besoins de la Défense.

Des technologies dont nous sommes encore loin d'avoir perçu tout le potentiel

« Avant qu'une arme nouvelle ne parvienne à son plein épanouissement, son emploi connaît plusieurs stades : le premier est celui d'auxiliaire modeste des armes en places. [...] Au deuxième stade de son développement, l'arme nouvelle est admise à l'intervention directe dans le combat [...]. Au troisième et dernier stade, [elle] s'est créée ses missions propres qui n'ont plus qu'un rapport indirect avec la conduite des opérations telle qu'on la concevait antérieurement à sa naissance » ⁽¹¹⁾.

(10) Robot convertible, multiples robots capables de se regrouper et de s'agréger en un seul...

(11) Camille ROUGERON, *Les enseignements aériens de la guerre d'Espagne*, Berger-Levrault, 1939.

S'il est difficile de prévoir *a priori* les usages de nouvelles technologies, cette difficulté est exacerbée pour la robotique et l'intelligence artificielle, dont les recherches foisonnent tous azimuts aujourd'hui. Il est par exemple frappant de constater que les concepts envisagés en France pour les futures applications militaires sont limités par rapport à l'ampleur des champs explorés par la recherche.

Les perspectives actuelles de robotique militaire, quand elles ne concernent pas une « niche » (contre-IED par exemple), sont pour l'essentiel fondées sur les technologies d'autonomie décisionnelle centralisée, sur les communications et la fusion des informations. Ce concept de robotique, prolongement naturel de nos plateformes de combat aux systèmes centralisés et mettant en œuvre de nombreux capteurs et effecteurs, est décrit par Peter W. Singer qui le nomme *Mothership*. Fondé sur la concentration de la puissance de feu, le pouvoir de décision repose sur des manœuvres mécaniques, l'allocation de ressources s'effectue en mode *point and click*.

À l'inverse, les réflexions sur les intelligences distribuées et les concepts d'essaim (*Swarm*) sont en France limitées à quelques recherches académiques (travaux sur les algorithmes de meutes de drones sous-marins par l'ENSTA Brest par exemple), alors que l'*US Air Force* expérimente déjà des démonstrateurs d'essaims d'une centaine de mini-drones aériens. Elles correspondent cependant à des tactiques militaires bien connues et à l'efficacité éprouvée : tactiques de guérilla employées par Lawrence d'Arabie, attaque en meute des convois de l'Atlantique par les *U-Boot*... Les caractéristiques militaires de ce concept d'essaim sont radicalement différentes du précédent (action d'ensemble pouvant être peu lisible par l'adversaire, flexibilité et robustesse intrinsèque aux pertes de combat, grande zone d'action, « mise à l'échelle », c'est-à-dire capacité à fonctionner quelle que soit sa taille...). Il en est de même des technologies nécessaires (robots moins sophistiqués, moins performants ou mono tâche, communications et moyens de détection locaux, limités aux drones voisins). Le développement important d'un concept similaire dans le domaine de l'observation spatiale (constellations importantes de microsatellites susceptibles de concurrencer les gros satellites d'observation traditionnels) devrait nous faire nous interroger sur la nécessité d'élargir la recherche à des concepts non traditionnels.

Ainsi, s'il n'est pas possible aujourd'hui de percevoir l'ampleur des apports de la robotique sur les capacités militaires, il est primordial de ne pas considérer le domaine comme un ensemble monolithique. Compte tenu du rythme actuel des progrès technologiques, il s'agit au contraire d'intégrer à nos réflexions la diversité des technologies émergentes. Se limiter aux applications les plus évidentes nous fait sinon courir le risque de passer à côté de futures « révolutions dans les affaires militaires ».

Des réticences et objections parfois infondées, sinon sujettes à débat

Pertinence des réticences morales ou éthiques ?

Les robots ne constituent pas des armes classiques opérées par l'homme : acteurs du champ de bataille, ils sont susceptibles de se substituer à un être humain.

L'autonomie décisionnelle et l'auto-apprentissage font par contre surgir le spectre d'une perte de contrôle.

La question du caractère immoral du développement et de l'acquisition de nouvelles armes s'est posée à plusieurs reprises au cours de l'histoire en Occident. L'interdiction de l'usage de l'arc et de l'arbalète en 1139 ⁽¹²⁾ ne fut aucunement respectée lors des conflits qui suivirent. De même, les prises de position des évêques d'Orléans et de Verdun en 1973 montrent que les oppositions à la dissuasion nucléaire continuèrent à être vives dix ans après sa mise en place en France, mais sans effet ⁽¹³⁾.

Il est peu probable que les débats actuels sur la limitation pour raisons morales des drones militaires, soupçonnés de déshumaniser la guerre, soient conclusifs, dès lors qu'une telle limitation, de même que pour l'arbalète, ne saurait être universelle. En effet, la question ne semble pas se poser en Orient par exemple, probablement du fait d'une distinction moindre entre les êtres animés et les objets inanimés. Le Shintoïsme et le Bouddhisme semblent en effet favoriser naturellement l'intégration des robots dans la société, ceux-ci faisant partie de l'ordre naturel des choses, faisant même parfois l'objet de rites funéraires. De plus, la prolifération des technologies étant inéluctable et renforcée par leur diffusion pour des applications civiles, une telle restriction s'opposerait à la justice ou l'équité, valeurs fondamentales de la morale. Enfin, il est curieux de constater qu'alors que le débat est intense sur les robots armés autonomes qui n'existent pas encore, il n'a jamais eu lieu véritablement concernant l'usage d'animaux – avéré ou potentiel – par les Russes (« chiens antichars » de la Seconde Guerre mondiale, « dauphins de combat » actuels).

En réalité, la qualité d'agent moral ne se pose pas pour le robot dès lors qu'on exclut l'hypothétique « Singularité » qui le doterait d'une conscience. D'un point de vue philosophique, même si le robot autonome peut sous certains aspects ressembler au mercenaire ou à l'animal domestiqué, il ne pourrait être maître de ses actes puisqu'il dépend de sa programmation. Il serait en outre incapable de l'empathie résultant de la transposition à autrui d'un instinct de survie, nécessaire pour générer une morale.

Sur la question de l'éthique, les débats actuels sont très intenses et focalisés aussi sur les Systèmes d'armes létaux autonomes (SALA), qualifiés de « robots tueurs ». À grand bruit, de nombreuses personnalités reconnues, incluant Elon Musk (Tesla, Space X, Hyperloop et OpenAI ⁽¹⁴⁾) et Stephen Hawking (physicien théoricien et cosmologiste britannique), ont demandé récemment leur interdiction. On peut évidemment s'interroger sur les raisons d'un tel geste, pouvant être motivé, par corporatisme des chercheurs roboticiens ou par mercantilisme des industriels du secteur, par une

(12) Concile de Latran II : « Nous défendons sous peine d'anathème que cet art meurtrier et haï de Dieu qui est celui des arbalétriers et des archers soit exercé à l'avenir contre des Chrétiens et des Catholiques. » (Canon 29).

(13) « Je me dois dans ma conscience d'homme, de chrétien et d'évêque [...] de dire non aux armes nucléaires [...] La France serait si grande si elle affirmait à la face du monde : j'ai le pouvoir de faire des expériences nucléaires et de posséder la bombe atomique : j'y renonce pour le bien de la paix. », cité par Marc TRONCHOT dans *Les présidents face à Dieu*, Calmann-Lévy, 2015.

(14) Association de recherche à but non lucratif en intelligence artificielle dont l'objectif est de promouvoir et développer une IA *open-source* bénéficiant à l'humanité.

volonté de ne pas freiner le développement de la robotique civile : les robots militaires pouvant lui conférer une image négative. Mais les arguments de fond invoqués sont également sujets à caution : la volonté d'éviter une nouvelle course aux armements est un vœu pieu ou susceptible de désavantager les États de droit, la robotique militaire n'ayant que peu de spécificités par rapport à la robotique civile. De même, bien que certains considèrent les robots comme une nouvelle catégorie d'armes de destruction massive – considérant qu'un niveau d'autonomie suffisant permettrait à un faible nombre d'opérateurs de provoquer des destructions importantes en dirigeant une myriade de robots – ce risque ne saurait être maîtrisé par une mise au ban. La facilité d'accès ne permet en effet pas d'appliquer les recettes qui sont efficaces en termes de lutte contre la prolifération nucléaire. Plus généralement, on peut s'interroger sur l'efficacité d'une interdiction dans un contexte de délitement du droit international (emploi de l'arme chimique en Syrie, annexion d'îlots en mer de Chine, remise en cause des frontières en Europe...).

Penser que le robot autonome puisse être un agent éthique serait également une erreur. Une vision anthropomorphique de l'éthique conduit en effet à exclure cette possibilité, le manque de créativité du robot ne lui permettant pas de sortir de sa programmation. Les règles prédéfinies seront toujours insuffisantes, de même que les lois n'ont pas fait disparaître le juge ⁽¹⁵⁾. Le robot ne serait ainsi pas immoral mais amoral, et aussi incapable d'éthique qu'une flèche ou qu'un missile.

Néanmoins, ceci ne signifie pas que le comportement des robots ne puisse pas être maîtrisé pour retranscrire la morale et l'éthique de leurs concepteurs. De nombreux travaux sont en cours ⁽¹⁶⁾, visant à la définition de réels algorithmes de gouvernance : leur complexité ira croissant au fur et à mesure qu'il faudra tenir compte d'environnements et de situations variés afin d'imiter plus fidèlement l'homme. En outre, les acteurs français de la recherche académique, incluant le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) et l'Office national d'études et de recherches aérospatiales (Onera), ont récemment proposé des modalités d'intégration des considérations liées à l'éthique dans les projets robotiques et ont mis en évidence le besoin de sensibiliser et d'accompagner les équipes de recherche sur le sujet. Cette stratégie apparaît préférable à l'imposition de règles ou normes éthiques qui seraient mal acceptées ou stérilisantes pour l'innovation. Elle pourrait être envisagée pour les projets de défense.

Les robots posent-ils des questions juridiques ?

Les travaux visant à la mise en place d'un cadre juridique spécifique pour les robots militaires ont débuté. Les débats se focalisent là aussi uniquement sur la question de l'interdiction des systèmes d'armes létaux autonomes, avec un engagement fort

(15) C. PERELMAN, citée par MdN RUFFO dans *Le robot, étranger de l'éthique*, indique que le droit n'est pas réductible à des règles : « il est nécessaire parfois renoncer à punir au bénéfice du doute ou renoncer à juger pour permettre le pardon qui conditionne la réconciliation ». Ainsi, la seule application par Salomon du principe d'équité aurait conduit à un assassinat bien moins moral, éthique et efficace que le résultat de sa créativité, de son intelligence affective et de son instinct.

(16) En particulier les travaux de Ronald ARKIN, professeur au *Georgia Institute of Technology*.

des organisations non gouvernementales (ONG) depuis plusieurs années en faveur d'une interdiction (en premier lieu *Amnesty International* et *Human Rights Watch*). Cette pression a conduit au lancement d'une réflexion informelle dès 2014 sous couvert de l'ONU, dans le cadre de la convention sur certaines armes classiques (*Certain Conventional Weapons* ou *CCW*). Fin 2016, un groupe d'experts a été officiellement créé pour deux ans. L'objectif visé et l'issue restent incertains : une vingtaine d'États se sont d'ores et déjà prononcés pour une réglementation internationale. Les membres permanents occidentaux du Conseil de sécurité quant à eux souhaitent orienter les travaux vers le partage des bonnes pratiques et la transparence sur les modalités de prise en compte des aspects juridiques dans l'acquisition des nouveaux armements.

Le premier problème posé par ces travaux est la possibilité de la mise en place d'un droit international *a priori* spécifique pour de nouvelles armes, ce qui serait une première. Encore très fantasmés, il est difficile d'anticiper ce dont seront réellement capables les robots autonomes militaires, quels seront leurs usages et les contextes dans lesquels nous pourrions ou devrions y avoir recours, avec le risque de mettre en place un droit inadapté. De même, la vitesse d'évolution du monde et le risque de résurgence de dangers inédits à l'horizon de 15 ans (horizon crédible de généralisation de certains types de robots militaires) incitent à la prudence et à relativiser l'intangibilité du droit par rapport aux circonstances ⁽¹⁷⁾.

La raison originelle invoquée par les ONG favorables à une interdiction est le manque actuel de clarté sur les chaînes des responsabilités dans l'emploi des robots armés, l'absence de responsabilité pouvant faciliter l'usage illégitime de la force voire les comportements inhumains ou non conformes aux règles du droit international. Or, il ne fait pas de doute que des clarifications seront rapidement apportées par le secteur civil, car elles sont nécessaires pour le développement des marchés, tel que celui des voitures autonomes (responsabilités entre le concepteur, le programmeur, le propriétaire, l'opérateur...). Il est possible d'ailleurs qu'elles s'inspirent du droit appliqué sur les dommages causés à autrui par les animaux de compagnie.

La nécessité de compléter le droit international est également discutable : rien ne permet pour l'instant d'affirmer avec certitude que le droit existant est insuffisant et il ne semble pas apparaître d'incompatibilité *a priori* entre les robots et le droit de la guerre (ou droit de La Haye ⁽¹⁸⁾) ou le droit humanitaire ⁽¹⁹⁾. Sous réserve d'une programmation adéquate, il n'y a pas d'obstacle technique insurmontable à l'implémentation des obligations de protection des civils et des combattants, et en particulier l'interdiction de « ne pas faire de quartier » ⁽²⁰⁾.

(17) On se souviendra que les Américains avaient cherché à interdire les attaques sous-marines des bâtiments civils (« guerre sous-marine sans restriction ») pendant l'entre-deux-guerres suite au choc provoqué notamment par la destruction du *Lusitania*. Ils n'ont pas hésité juste après l'attaque de Pearl Harbour à ordonner la destruction de la flotte marchande du Japon, pour accélérer le renversement du rapport de force dans le Pacifique.

(18) Regroupe l'ensemble formé par les Conventions de La Haye, dont les plus connues sont celles du 18 octobre 1907 concernant d'une part les lois et coutumes de la guerre sur terre, et d'autre part la pratique de la guerre maritime.

(19) Ensemble formé par les conventions de Genève du 12 août 1949 concernant les blessés et malades (1^{re} convention), les naufragés (2^e convention), les prisonniers de guerre (3^e convention) et la population civile (4^e convention).

(20) Peter W. STINGER, dans *Wired for war*, cite d'ailleurs le premier cas de reddition face à un drone pendant la guerre du Golfe : un *Pioneer* lancé de l'*USS Wisconsin* obtint la reddition des troupes irakiennes basées sur l'île de Failaka.

Certains auteurs vont même au-delà. Plutôt que de voir les robots comme un problème possible pour le respect du droit international, certains mettent au contraire en avant des avantages indéniables en termes de respect des trois principes fondamentaux des conflits armés : humanité, discrimination et proportionnalité. On peut en effet considérer que les robots sont plus précis et prédictibles que l'homme, ne connaissent pas l'esprit de vengeance. Ils pourront être astreints à des règles d'engagement plus contraignantes que les hommes (par exemple n'ouvrir le feu qu'en riposte, même si cela conduit à un risque de perte plus élevé), ils disposeront de capacités sensorielles supérieures à l'homme (caméras numériques avec zoom de grande performance, caméras thermiques...).

Quant à la question de l'impossibilité pour un robot d'appliquer « le principe d'humanité dans l'acte de guerre » (clause dite de Martens ⁽²¹⁾), elle dépasse largement le seul champ juridique et doit être considérée sous l'angle philosophique, de la psychologie ainsi que des neurosciences. Le débat ne peut se limiter à ne voir que l'inhumanité du robot sans aborder également l'humanité de l'être humain lui-même. Les écrits d'Hannah Arendt à la suite du procès d'Eichmann ⁽²²⁾, les comptes rendus des expériences de Milgram ⁽²³⁾ ou de Stanford ⁽²⁴⁾ mettent en évidence la relativité de l'humanité de l'individu et de sa capacité à distinguer le bien du mal, en particulier dans des contextes autoritaires, agressifs ou en situation de stress. Ils relativisent le risque de « bulle de technologisation » qui serait susceptible de conduire à des comportements immoraux, conscients ou non, par les opérateurs de robots ⁽²⁵⁾. À l'extrême, le robot pourrait même être considéré comme un rempart contre l'inhumanité : surveillant l'homme combattant à côté de lui, il pourrait le dissuader d'avoir des comportements déviants pouvant être liés aux traumatismes subis pendant l'action (pertes amies, stimuli...).

Les robots facteurs de banalisation de la guerre, et d'augmentation de la violence ?

Les effets des innovations technologiques dans le domaine de l'armement ne se limitent pas aux affaires militaires mais transforment également les relations internationales, les sociétés. De Cortes à Lyautey, la poudre et la mécanisation ont ainsi été décisives pour les colonisations. L'arme nucléaire a été au centre des relations Est-Ouest de l'après-guerre. Les nouveaux armements peuvent dissuader de la guerre, mais aussi inciter à la déclarer.

(21) « Les personnes civiles et les combattants restent sous la sauvegarde et sous l'emprise des principes du droit des gens, tels qu'ils résultent des usages établis, des principes de l'humanité et des exigences de la conscience publique. »

(22) La philosophe Hannah ARENDT décrira dans *Eichmann à Jérusalem. Rapport sur la banalité du mal*, l'obéissance aveugle dont a fait preuve l'homme et comment l'instauration du régime nazi a été permise par la destruction de la volonté individuelle, mettant en avant la responsabilité collective du régime plutôt que la responsabilité individuelle de l'accusé.

(23) Ces expériences sur la soumission à l'autorité ont été conduites en 1963 par le psychologue Stanley Milgram. Deux tiers des volontaires ont obéi aux ordres, jusqu'à envoyer des décharges mortelles à une personne sans défense (en fait un acteur).

(24) L'expérience de Stanford (effet Lucifer) est une étude de psychologie expérimentale menée par Philip Zimbardo en 1971 sur les effets de la situation carcérale. Elle fut réalisée avec des étudiants qui jouaient des rôles de gardiens et de prisonniers. L'une des conclusions de l'étude est qu'un tiers des gardiens fit preuve de comportements sadiques.

(25) Expression attribuée à Joseph HENROTIN, cité par Tristan ZELLER dans « Les robots militaires sont là... et maintenant ? », *Pensée mili-terre* (CDEC), 2015.

Les ONG hostiles aux robots, mais également certains auteurs, pointent que les robots sont une nouvelle étape dans l'éloignement progressif entre l'armée et la nation qui s'est amplifié depuis la professionnalisation, entraînant par rebond une distanciation du politique. Ils considèrent que celui-ci serait alors plus enclin à décider de l'usage de la force armée, décision plus facile et moins risquée politiquement compte tenu de la réduction du risque de perte humaine. La guerre se verrait en quelque sorte vidée de sa signification politique, banalisée : l'armée ne serait plus l'*ultima ratio*. Ces raisonnements, théoriques car fantasmant une hypothétique armée totalement robotisée, apparaissent totalement déconnectés de la réalité : les armées n'ont eu de cesse d'utiliser la technologie pour proposer au politique des modes d'action permettant d'éviter les pertes et d'opérer le plus impunément possible : les vols de *U-2* au-dessus de l'URSS auraient-ils eu lieu si l'avion n'avait pas été hors de portée des défenses ? La France aurait-elle planifié une frappe de missiles de croisière en Syrie en 2013 en rétorsion à l'usage d'armes chimiques si le risque de perdre des pilotes avait été important ? La robotique militaire ne changera pas la nature de la guerre, qui restera un choc des volontés ; par contre les robots nous permettront de conserver notre liberté d'action, en limitant le risque de pertes amies.

Dans le cadre d'engagements asymétriques, il est souvent évoqué par les détracteurs que l'effet sur l'ennemi des robots serait délétère pour notre population, en reportant sur elle les attaques d'un ennemi vengeur devenu impuissant à nous occasionner des pertes. Il est aussi reproché que l'efficacité de l'action militaire serait amoindrie par la robotique, compte tenu de l'image de lâcheté qu'elle véhiculerait, incitant l'ennemi à poursuivre le combat. Antonin Tisseron souligne que cette idée est depuis longtemps utilisée dans la propagande des Talibans et de leurs alliés. C'est faire un faux procès aux robots : l'adversaire asymétrique est déjà impuissant contre nos drones et avions de chasse, et nous n'avons de cesse d'améliorer le blindage de nos véhicules. En réaction, il déploie d'ores et déjà des modes d'action terroristes, tant contre les forces sur le terrain que contre les populations civiles. Encore une fois, ce n'est pas aux robots qu'il faut attribuer ces risques mais à notre modèle occidental de supériorité technologique. En engagement asymétrique, le robot est la continuation d'un modèle créant entre nous et notre adversaire les conditions d'une asymétrie du risque (pertes matérielles encourues contre pertes humaines), indispensable pour ne pas être amené à l'inaction quand il y a asymétrie des enjeux (expédition extérieure contre guerre existentielle).

Dans le cadre d'engagements symétriques, les robots augmenteront la résilience de notre volonté tout en diminuant celle de l'ennemi. Un belligérant équipé de robots disposera en effet d'avantages décisifs face à son adversaire qui verrait son potentiel militaire plus durablement atteint par les pertes, mais également sa volonté et son moral plus durement ébranlés par les pertes humaines consenties jugées de valeur bien supérieures aux pertes matérielles occasionnées.

La question qui reste à traiter sur l'impact au niveau stratégique de la robotique est son effet sur le règlement des conflits. Les robots, seuls, seront en effet incapables de « gagner la paix », dès lors que le centre de gravité ennemi sera le soutien que lui apporte la population locale et qu'il s'agira de gagner « les cœurs et les esprits ». Dans

le cadre des opérations de contre-insurrection, l'effet de distanciation créé par rapport à la population peut être contre-productif.

Nos réflexions sur la place des robots au sein des capacités militaires devront ainsi tenir compte de la nécessité de conserver le point fort du modèle français qui place depuis longtemps le contact humain et le soldat au centre de la guerre « au sein des populations ».

Piloter la transformation et maîtriser les risques

L'introduction d'une part croissante d'éléments robotiques dans nos capacités militaires est inéluctable et a déjà débuté. Il en sera de même de l'intelligence artificielle, indispensable pour limiter le besoin en servants et dès lors que la charge cognitive sera trop importante pour l'homme, les temps de réflexion trop contraints ou qu'il sera nécessaire de pallier la vulnérabilité aux communications (vulnérabilité des systèmes au déni de spectre électromagnétique).

Pour se préparer à cette transformation, une réflexion globale doit être conduite. Les éléments ci-après portent sur les axes de travail apparus, à l'issue de l'étude menée, les plus urgents à ouvrir, sans souci d'exhaustivité ni prétention que d'autres questions d'importance supérieure puissent résulter d'une analyse plus approfondie.

Il apparaît en premier lieu nécessaire de rassurer et lever les réticences initiales naturelles, en maîtrisant les vulnérabilités nouvelles et en objectivant la place à laisser pour l'homme, dans un esprit de complémentarité. Il sera également nécessaire de créer les conditions favorables au développement des futures capacités robotisées, d'adapter nos méthodes et d'intégrer les nouveaux acteurs nécessaires.

Anticiper et se prémunir des vulnérabilités (ou des limitations)

Le risque d'une perte de contrôle des systèmes numériques est réel. Celle-ci peut être le fait d'une action de l'adversaire, tel que le détournement en 2007 par les Tamouls d'un satellite *Intelsat*. Elle peut également être involontaire, liée à une erreur humaine comme cela était le cas lors de plusieurs alertes nucléaires américaines dans les années 1970-1980 ⁽²⁶⁾, ou bien résulter d'un manque de maîtrise de la technologie, illustré par les dérives d'un *chatbot* de Microsoft en 2016 ⁽²⁷⁾.

L'enjeu sera, au-delà de la mise en place de dispositifs de protection comme cela est fait classiquement, de chercher à limiter les effets d'un inéluctable piratage ou *bug*. Dès la conception, la possibilité de barrières physiques sur le robot pourra être envisagée (limitations sur le rayon d'action, la vitesse ou la charge utile par exemple). De même que pour la programmation de règles éthiques ou juridiques, des algorithmes

(26) Alan BORNING, dans *Computer System Reliability and Nuclear War*, évoque notamment qu'en 1979 un programme de simulation fut accidentellement chargé dans le système d'alerte du *NORAD*, ayant amené à la mise en vol des bombardiers stratégiques.

(27) Le robot conversationnel expérimental *Tay* de Microsoft a tenu sur *Internet* des propos racistes, sexistes et anti-sémites qui lui ont été appris de l'interaction avec les internautes.

de gouvernance pourront aussi limiter les actions ou cadres d'emploi autorisés en implémentant des règles d'engagement, y compris pour les systèmes à forte autonomie. Ces règles pourront être simples (inaction en situation non connue ou conforme, action limitée aux véhicules ou systèmes d'armes, tir uniquement en riposte, *kill boxes*...) ou plus complexes (à l'exemple des trois lois de la robotique définies par l'auteur de science-fiction Isaac Asimov⁽²⁸⁾).

Au-delà des robots physiques, cette logique de limitation des effets non désirés pourrait être à appliquer également aux logiciels opérationnels. En effet, les systèmes d'intelligence artificielle se développeront également dans les systèmes d'information et les logiciels d'aide à la décision. Il conviendra d'être vigilant sur la gravité des risques encourus en cas de mauvais fonctionnement voire, si nécessaire, de limiter volontairement l'interconnexion des réseaux pour limiter l'impact.

Le niveau de souveraineté à atteindre sur les intelligences artificielles doit également être défini. Si cela s'avérait nécessaire, l'internalisation d'une partie de la recherche et technologie (R&T), voire la réalisation de certains développements en interne au sein du ministère de la Défense pourrait s'avérer nécessaire (comme c'est le cas à DGA/Maîtrise de l'Information pour une partie des activités de cyber).

Définir la place de l'homme

Le combattant humain ne va pas disparaître. En revanche, le monopole des actions de guerre, incluant le droit de vie et de mort, sera à l'avenir partagé entre l'homme et le robot. Ceci amène le militaire à des réticences naturelles pouvant conduire au rejet. Cette évolution pourrait aussi être perçue comme une contestation de sa « légitimité qui s'appuie sur une spécificité : le militaire se doit au final de mettre sa vie en jeu »⁽²⁹⁾. Si cette question de la place laissée au militaire est exacerbée quand il s'agit de robots, on pourra néanmoins noter qu'elle se pose déjà avec l'importante « civilianisation » de domaines tels que le renseignement.

Afin d'objectiver cette question et sortir de l'émotion, un audit global des métiers et fonctions au sein des armées permettrait de définir et distinguer, à l'instar des études réalisées dans l'industrie, ceux qui pourraient être remplacés par des robots de ceux qui devront s'adapter à leur présence. Se poser la question systématique de la possible robotisation permettra de faire émerger les places et les fonctions pour lesquelles l'homme est indispensable.

La catégorisation est parfois assez intuitive : une partie des fonctions de reconnaissance semble déjà faire partie de la première catégorie (drones) de même que certains métiers de la logistique, très similaires à des métiers du civil en cours de transformation (fret, manutention...). *A contrario*, une place devra être préservée pour

(28) « Un robot ne peut blesser un être humain ni, par son inaction, permettre qu'un humain soit blessé » ; « Un robot doit obéir aux ordres donnés par les êtres humains, sauf si de tels ordres sont en contradiction avec la 1^{re} loi » ; « Un robot doit protéger sa propre existence aussi longtemps qu'une telle protection n'est pas en contradiction avec la 1^{re} et/ou la 2^e Loi ».

(29) Philippe VIAL, professeur au CHEM lors d'une conférence sur les relations politico-militaires.

l'homme pour les opérations spéciales (adaptabilité) et pour les opérations de contre-insurrection (au contact des populations).

Dans le domaine des systèmes d'aide à la décision, si des fonctions tactiques, souvent au champ d'action restreint, seront probablement numérisables, des limites existeront pour les outils de planification opérationnelle ou d'aide à la décision. En effet, il s'agira de ne pas être prévisible et de conserver la créativité nécessaire pour appréhender des contextes toujours très différents, des situations inédites, ce qui est peu compatible avec l'auto-apprentissage⁽³⁰⁾.

Un audit sur les activités humaines devra également permettre de mettre en évidence les niveaux d'autonomie à viser pour les robots, en fonction des domaines. Cette démarche devra être conduite sans tabou. Si la place de l'homme en supervision est un objectif général à rechercher, celui-ci ne sera un jour plus pertinent confronté à de nouvelles armes trop rapides, trop nombreuses ou opérant dans un environnement trop complexe : bien que les doctrines actuelles française ou américaine soient de conserver l'homme dans la boucle pour la décision de vie ou de mort⁽³¹⁾, il est peu probable que cette limite reste en place lorsque le tempo de l'engagement sera incompatible avec la vitesse de réflexion.

Travailler la complémentarité homme-robots

La complémentarité entre le robot et le soldat est au cœur de la stratégie américaine du Centaure. Celle-ci met en avant le contrôle par l'homme, secondé par des armes autonomes lui permettant de se concentrer sur ses points forts par rapport au robot : le bon sens, la créativité, les capacités de résolution de problème et d'adaptation (les intelligences artificielles semblent avoir des difficultés pour accomplir les tâches que les hommes – ou les animaux – réalisent sans réfléchir...). Il ne s'agirait donc pas de remplacer l'homme mais de le placer au centre, d'exploiter l'efficacité tactique du robot pour augmenter l'ingéniosité stratégique humaine. Ce concept du Centaure doit permettre, en outre, de tirer parti de l'avantage des armées occidentales, en faisant la synthèse entre supériorité technologique et supériorité dans la subsidiarité des chaînes de commandement, à comparer aux systèmes très centralisés des armées russes ou chinoises.

Un autre élément majeur de complémentarité homme-robot est la différence de rapport au temps entre l'homme et la machine. Si au niveau tactique la fulgurance est un atout, ce n'est pas nécessairement le cas au niveau stratégique ou politique où la lenteur humaine peut être un avantage. Le risque d'emballement d'intelligences artificielles, en particulier si elles sont mises en réseau, est incompatible avec la possibilité

(30) Cette probable dichotomie tactique fortement automatisable/stratégique peu automatisable peut être illustrée par une citation de TALLEYRAND : « Je crains plus une armée de cent moutons commandée par un lion qu'une armée de cent lions commandée par un mouton ».

(31) La directive *Autonomy in Weapon Systems* de 2012 du DoD indique que les systèmes autonomes doivent être conçus pour permettre aux opérateurs d'exercer la sélection des cibles, y compris en posture défensive : « *exercise appropriate levels of human judgement over the use of force* ». En France, les réticences portent sur le remplacement de l'homme dans les phases d'orientation et de décision de la boucle OODA (Observer – Orienter – Décider – Agir).

d'éviter l'escalade de la violence. Il peut également être plus efficace, dans le souci qui doit être constant de « gagner la paix » (et non uniquement la guerre), d'octroyer une pause pour l'action diplomatique, voire de renoncer temporairement à la force brutale ou faire preuve de compassion pour l'adversaire. Dans ces moments décisifs pour la suite des opérations ou le règlement d'un conflit, conserver l'homme au centre est nécessaire.

Faciliter l'acceptabilité

L'inconscient collectif occidental est alimenté par les œuvres de science-fiction bien souvent associées à des catastrophes liées à la perte de contrôle des robots par l'homme, malgré ses efforts pour définir des règles, par accident ou naïveté (films *Wargames*, saga *Terminator*...). Mais ceci n'est pas spécifique des robots : la technologie en général est souvent présentée comme le facteur de supériorité du « méchant » (dans *Star Wars* la technologie est dans le camp de l'Empire et les valeurs humaines dans celui de la rébellion).

La communication peut contribuer à compenser cette « peur de la modernité », survenue à de nombreuses reprises dans l'histoire des technologies. Afin de faciliter l'acceptabilité des robots militaires, les acteurs étatiques et industriels de la défense pourront intégrer dans leurs projets de robotique une analyse des effets sociétaux sur l'opinion publique et des actions (de communication, maîtrise de l'impact dans le champ des perceptions : iconographie, forme et apparence des robots...) qui permettent de faciliter l'acceptation. Des réflexions sont déjà en cours au sein du Gifas⁽³²⁾.

À court terme, comme le demandent également de nombreuses voix pour des raisons d'efficacité opérationnelle et d'économie des moyens, l'intégration d'un armement aux drones français actuellement en service, bien que ceux-ci ne présentent aucun niveau d'autonomie, contribuerait également à faire accepter les robots militaires, par effet progressif d'accoutumance.

Enfin, comme le constate Antoine Petit, PDG de l'Institut national de recherche en informatique et en automatique (Inria), l'informatique souffre d'une illusion de familiarité – « tout le monde maîtrise *Windows* » – qui limite le recours au spécialiste, nécessaire pour élaborer des avis et opinions éclairées. Le problème est accentué pour l'intelligence artificielle, qui pâtit d'une difficulté à l'expliquer qui croît en même temps que ses performances. Des actions d'information et de vulgarisation seraient utiles, notamment vers les décideurs, mais la question dépasse largement la seule sphère de la défense. Le vocabulaire pourrait déjà être adapté, en substituant la notion positive de « délégation d'autorité » (utilisée pour les voitures autonomes) à l'« intelligence artificielle », qui nous ramène trop facilement aux thèses des trans-humanistes avec les craintes associées.

(32) Gifas : Groupement des industries françaises aéronautiques et spatiales. Cité par Éric GERMAIN dans « Drones : l'impératif stratégique de la prise en compte des enjeux éthiques et sociétaux », *Penser les ailes françaises* n° 29, avril 2013.

Réfléchir plus large et en amont, en intégrant réflexions doctrinales et recherches

La démarche capacitaire suit actuellement une révolution à travers la mise en place du processus de « maîtrise de l'architecture du système de défense » (MASD), sous l'impulsion de la DGA et avec le soutien de l'EMA. La complexité accrue liée à l'interconnexion généralisée des systèmes d'information et systèmes d'armes, de leur utilisation dans des contextes de plus en plus « inter- » (armes, armées et alliés dans le cadre de coalitions de circonstance) a conduit à la mise en place de méthodes de travail collaboratives entre les états-majors et la DGA, en associant l'industrie. L'analyse poussée des chaînes fonctionnelles et le recours accru à la simulation sur des scénarios doivent permettre de réaliser des optimisations globales de l'outil militaire – au sein du système de défense – et non plus locales – au niveau d'un programme d'armement individuel. En parallèle, pour favoriser l'intégration de l'innovation dans les systèmes militaires, sont mis en place des *Labs* destinés à confronter utilisateurs, acheteurs, *Start-up* et PME, ainsi que grands industriels.

Malgré ces actions de travail collaboratif et de réseau, le hiatus restera toujours important entre les travaux capacitaires, la réflexion doctrinale et la recherche. Même les réflexions opérationnelles les plus poussées restent empreintes de prudence : l'objectif de l'État-major de l'Armée de terre sur les robots autonomes à l'horizon d'une quinzaine d'années n'a pas d'équivalent dans les autres armées ; il reste néanmoins modérément ambitieux (il s'agit de mieux protéger le combattant, en priorité « améliorer le renseignement de contact, le traitement des engins explosifs improvisés et mines, renforcer les capacités de destruction du combattant et l'alléger »).

La mise en place d'un espace de travail collaboratif intégrant, dans le cercle des acteurs de la préparation des futures capacités et architectures, le monde de la recherche et les organismes de doctrine des armées permettrait de ne pas passer à côté de technologies susceptibles de constituer des game changer ou de ne pas manquer la doctrine innovante permettant de tirer profit d'une innovation (à l'instar de la *Blitzkrieg* avec les chars avant guerre).

Le concept d'essaim de robots est illustratif des révolutions doctrinales potentielles peu approfondies en France aujourd'hui, qui mériteraient d'être plus vivement explorées : l'*USAF* expérimente le largage d'essaims car ce concept pourrait changer la donne du combat aéroterrestre et permettre l'intervention de la force aérienne dans le combat urbain. Fondés sur des robots peu sophistiqués unitairement, les essaims pourraient également être une voie pour nous dégager de l'augmentation continue du coût des systèmes (loi d'Augustine⁽³³⁾). Pour tirer le meilleur parti de la révolution robotique dont les limites, ni les voies, ne sont pas encore tracées, la démarche capacitaire doit permettre aux réflexions de s'étoffer et à la pensée militaire de « sortir de la boîte ».

(33) Selon Norman AUGUSTINE, ancien directeur de Lockheed Martin, si les budgets de défense évoluent linéairement, le coût unitaire des matériels croît exponentiellement : « *In the year 2054, the entire defense budget will purchase just one tactical aircraft. This aircraft will have to be shared by the Air Force and Navy 3½ days each per week except for leap year, when it will be made available to the Marines for the extra day.* ».

En termes d'organisation, un modèle de type *Defense Advanced Research Projects Agency (DARPA)* pour conduire des projets très innovants est une voie possible. Le sujet, régulièrement remis sur le devant de la scène, nécessiterait un effort humain et budgétaire important pour un pays comme la France. Plus modeste, la création d'une *task force* d'innovation pluridisciplinaire associant armées, ingénieurs et académiques, s'appuyant sur le DGA Lab, pourrait définir et explorer des concepts innovants, inventer puis surtout perfectionner les doctrines associées ⁽³⁴⁾.

Se préparer à un élargissement de la pluridisciplinarité dans les équipes de projets

L'effet à court ou long terme des robots sur les servants n'est pas anodin et dépasse largement les études d'ergonomie actuelles. Les risques émotionnels liés à l'interaction homme-robot font actuellement l'objet d'études approfondies avec la perspective du développement des robots domestiques ⁽³⁵⁾. Ils commencent à être pris en compte dans le monde militaire ⁽³⁶⁾ : l'utilisateur peut s'attacher au robot et ce lien affectif est de nature à affecter son efficacité. L'exemple est également connu des pilotes de drones américains subissant des troubles liés à la déconnexion d'avec leur vie quotidienne (le déploiement par l'Armée de l'air française des équipages de drones sur le théâtre *Barkhane* permet aujourd'hui de s'en prémunir).

Au-delà de l'empathie, d'autres phénomènes psychologiques devront être pris en compte. L'interaction avec les ordinateurs et les robots peut générer une perte du discernement, l'opérateur n'étant plus en mesure de contester l'autorité du système, remettant ainsi en cause le rôle de l'homme en « garde-fou », « dans la boucle ». L'exemple le plus utilisé pour illustrer ce phénomène est la destruction en 1988 d'un avion d'Iran Air par l'*USS Vincennes* : le système n'était pas en mode automatique mais, sous la pression, l'équipage n'aurait pas remis en cause l'information erronée, incohérente avec d'autres, par confiance excessive envers le système *AEGIS*.

Ces biais cognitifs font l'objet de recherches qui montrent que des solutions existent pour les limiter ⁽³⁷⁾ et « permettre à l'homme de continuer à raisonner et non uniquement d'observer » ⁽³⁸⁾. Il conviendra d'être vigilant sur ces biais alors que robots et systèmes informatiques experts se répandront (en particulier les aides à la décision). Pour certaines opérations d'armement, l'intégration d'un spécialiste de la psychologie humaine ou des neurosciences pourrait être pertinente. Un premier pas a été franchi dans le cadre du programme *Scorpion* pour lequel des études ont été conduites pour définir et maîtriser les niveaux de délégation d'autorité des nouvelles fonctions de combat collaboratif, en particulier quand elles étaient semi-automatiques.

(34) L'utilisation de l'arc long à Crécy en 1346 résultait du perfectionnement de doctrines utilisées auparavant lors de la guerre d'indépendance de l'Écosse. La portée de l'arc long permettait d'attirer l'adversaire en terrain défavorable et de le contraindre à attaquer une position fortifiée au préalable.

(35) Ce phénomène a été notamment illustré dans le film français *Ma vie avec un robot* de Thibault SÈVE et Emmanuel DUMONT.

(36) L'étude la plus souvent citée, par exemple par Patrick LIN dans le magazine *Forbes*, a été réalisée par Julie Carpenter de l'Université de Washington, et portait sur la relation complexe entre un soldat et un robot démineur.

(37) Une étude récente financée par l'Union européenne et publiée par le CEIS étudie ces biais pour les métiers du renseignement.

(38) Entretien avec Véronique SERFATY.

Conclusion

Les perspectives offertes par la robotique et l'intelligence artificielle sont telles qu'il ne fait pas de doute qu'elles vont se diffuser rapidement et largement. Une prise de conscience est nécessaire en France au sein de la Défense pour ne pas se faire dépasser et passer à côté de cette nouvelle « révolution dans les affaires militaires », probablement encore plus profonde que les précédentes.

Ne pas répéter les erreurs du passé dans une approche conservatrice nécessite une mobilisation des acteurs traditionnels de la préparation des futures capacités, mais également d'inclure de nouveaux intervenants. Des stratégies globales doivent être élaborées pour se préparer à la guerre de l'ère robotique, que le secrétaire de la Défense adjoint Bob Work prédit « avant 10 ans »⁽³⁹⁾.

Le moment est opportun en France et en Europe pour cette prise de conscience et cette mobilisation, alors que la question de l'adaptation de la société à la transformation numérique vient de faire irruption dans la campagne présidentielle ainsi qu'au Parlement européen. Une telle démarche s'inscrirait également en cohérence avec l'initiative *France IA* lancée en janvier dernier par les secrétaires d'État chargés de l'Innovation et du Numérique ainsi que de l'Enseignement supérieur et de la Recherche, visant à définir les grandes orientations de la France en matière d'intelligence artificielle, et dont les résultats sont attendus au printemps.

En parallèle, il sera nécessaire de mettre en place une communication stratégique pour sensibiliser l'opinion publique et lui faire comprendre que nous ne cherchons pas à faire émerger *Frankenstein* ou *Terminator*, mais visons à préparer l'armée et donc la Nation aux conflits de demain. L'appel de Vladimir Poutine début 2017 pour la création en Russie de complexes industriels destinés à développer la robotique autonome militaire⁽⁴⁰⁾ est symptomatique du tournant que nous devons collectivement prendre dans notre manière d'appréhender la robotique militaire.

(39) « *10 years from now if the first person through a breach isn't a friggin' robot, shame on us.* » (discours du 7 novembre 2015).

(40) « Retour vers le futur : Poutine a déclaré l'ère des robots militaires », Portail russe *Rambler.ru*, janvier 2017.

Robots et intelligence artificielle : quelle place pour l'homme dans les futures capacités militaires françaises ?

Éléments de bibliographie

Ouvrages

- ARENDRT Hannah, *Eichmann à Jérusalem*, Folio histoire, 1991, 512 pages.
- ASIMOV Isaac, *Les Robots*, J'ai Lu, 1973.
- COLLECTIF, *Robots on the Battlefield: Contemporary Issues and Implications for the Future*, Combat Studies Institute Press, 2014, 260 pages.
- MALIS Christian, *Guerre et stratégie au XXI^e siècle*, Fayard, 2014, 352 pages.
- SCHWAB Klaus, *La quatrième révolution industrielle*, Dunod, 2017, 208 pages.
- SINGER P.W., *Wired for War: Robotic Revolution and Conflict in the 21st Century*, Penguin, 2009, 512 pages.

Films et vidéos

- FORUM ÉCONOMIQUE MONDIAL, *What if robots go to war?*, 2016, 57 min
(www.youtube.com/watch?v=opZR7vLhXVg).
- SÈVE Thibault et DUMONT Emmanuel, *Ma vie avec un robot* (documentaire), 2015, 1 h 25 min.

Rapports et documents officiels

- ALLIANCE DES SCIENCES ET TECHNOLOGIES DU NUMÉRIQUE (ALLISTENE), *Éthique de la recherche en robotique, Rapport n° 1 de la CERNA* (Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene), novembre 2014, 60 pages
(http://cerna-ethics-allistene.org/digitalAssets/38/38704_Avis_robotique_livret.pdf).
- COLLECTIF, *Campaign to stop killer robots*, 2014 (www.stopkillerrobots.org/).
- DEPARTMENT OF DEFENSE (DoD), *Autonomy in Weapon Systems*, 21 novembre 2012
(<https://cryptome.org/dodi/dodd-3000-09.pdf>).
- HUMAN RIGHTS WATCH, *Losing Humanity: The Case Against Killer Robots*, novembre 2012, 50 pages
(www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf).
- HUMAN RIGHTS WATCH, « Mind the Gap: the Lack of Accountability for Killer Robots », 9 avril 2015
(www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots).
- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (Inria), *Intelligence artificielle : les défis actuels et l'action d'Inria (Livre blanc)*, septembre 2016, 82 pages
(www.inria.fr/actualite/actualites-inria/livre-blanc-sur-l-intelligence-artificielle).
- NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, *The National Artificial Intelligence Research and Development Strategic Plan*, octobre 2016, 40 pages (<https://obamawhitehouse.archives.gov/>).
- OCDE, *Automatisation et travail indépendant dans une économie numérique*, 2016, 5 pages (www.oecd.org/fr/).

Revue

- ABDUL-RAHIM Rasha, « 10 raisons pour lesquelles il faut interdire les robots tueurs », 12 novembre 2015
(www.amnesty.org/fr/latest/news/2015/11/time-to-get-serious-about-banning-killer-robots).
- ARKIN Ronald, « Ethical Robots in Warfare », IEEE Technology and Society magazine, mars 2009, 3 pages
(www.cc.gatech.edu/ai/robot-lab/online-publications/arkin-rev.pdf).
- ARKIN Ronald, « The Case for Ethical Autonomy in Unmanned Systems », *Journal of Military Ethics*, vol. 9 n° 4, octobre 2010, p. 332-341 (<https://smartertech.gatech.edu/>).
- BELKAAB Omar, « La Chine va investir plus de 13 Md€ dans l'intelligence artificielle », Numerama, 26 mai 2016
(www.numerama.com/).
- BENI Gerardo, « From Swarm Intelligence to Swarm Robotics » in *Swarm Robotics*, 17 juillet 2004, p. 1-9
(https://link.springer.com/chapter/10.1007/978-3-540-30552-1_1).
- BORNING Alan, « Computer System Reliability and Nuclear War », *Communications of the ACM*, vol. 30 n° 2, février 1987 (www-ee.stanford.edu/~hellman/Breakthrough/book/chapters/borning.html).
- « Véhicules autonomes : liste des entreprises actives - Voiture autonome », *Voiture autonome*, octobre 2016
(www.voiture-autonome.net/constructeurs/liste-vehicules-autonomes-604.html).
- CHIVA Emmanuel, « Un essaim de drones démontre des capacités de coordination », *VMF 214*, 17 janvier 2017
(<https://vmf214.net/2017/01/17/un-essaim-de-103-drones-aeriens-demontre-des-capacites-de-coordination/>).

Robots et intelligence artificielle : quelle place pour l'homme dans les futures capacités militaires françaises ?

- CLANSMAN, « AAI Q-2 Pioneer », *Aviationsmilitaires.net*, avril 2015 (www.aviationsmilitaires.net/v2/base/view/Model/1412.html).
- COLLECTIF, « Autonomous Weapons: an Open Letter from AI & Robotics Researchers », juillet 2015 (<https://futureoflife.org/open-letter-autonomous-weapons>).
- COLLECTIF, « Série robotique – 2 – Les robots militaires peuvent-ils adopter une éthique ? », *ParisTech Review*, 24 juin 2014 (<http://parisinnovationreview.com/2014/06/24/serie-robotique-robots-militaires-ethique/>).
- DORIGO Marco, BIRATTARRI Mauro et BRAMBILLA Manuele, « Swarm robotics », *Scholarpedia*, 2014 (www.scholarpedia.org/article/Swarm_robotics).
- DYÈVRE Axel, « Renseignement, facteur humain et biais cognitifs - Gnothi seauton », *Les notes stratégiques*, CEIS, juin 2015, 46 pages (www.sia-lab.fr/sites/sia/files/images/note_strat_-_renseignement_et_facteur_humain.pdf).
- FREEDBERG Sydney, « Centaur Army: Bob Work, Robotics, & The Third Offset Strategy », *Breaking Defense*, 9 novembre 2015 (<http://breakingdefense.com/2015/11/centaur-army-bob-work-robotics-the-third-offset-strategy/>).
- GADY Franz-Stefan, « New US Defense Budget: \$18 Billion for Third Offset Strategy », *The Diplomat*, 10 février 2016 (<http://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/>).
- GERMAIN Éric, « Drones : l'impératif stratégique de la prise en compte des enjeux éthiques et sociétaux », *Penser les ailes françaises* n° 29, avril 2013, p. 19-21 (www.cerpa.air.defense.gouv.fr/images/pdf/Plaf/PLAF29.pdf).
- GOFFI Emmanuel, « Robots de combat et morale : anticiper la responsabilité », *Penser les ailes françaises* n° 29, avril 2013, p. 28-40 (www.cerpa.air.defense.gouv.fr/images/pdf/Plaf/PLAF29.pdf).
- GROS Philippe, « La Third Offset Strategy américaine », *Défense & Industries* n° 7, juin 2016, p. 17-19 (www.frstrategie.org/publications/defense-et-industries/web/documents/2016/7-6.pdf).
- GUILLERMARD Véronique, « Patrice Caine : "Thales appelle à créer une grande agence de recherche avancée" », *Le Figaro*, 28 février 2017 (www.lefigaro.fr).
- HUTT Rosamond, « The US used to be the world leader in this key area of artificial intelligence research. Now it's China », *World Economic Forum*, 22 novembre 2016 (www.weforum.org/).
- JAESA, « La singularité technologique : en route vers le transhumain », 1^{er} mai 2015 (<https://iatranshumanisme.com/2015/05/01/la-singularite-technologique-en-route-vers-le-transhumain/>).
- JEANGÈNE VILMER Jean-Baptiste, « Introduction : robotisation et transformations de la guerre », *Politique étrangère* n°3/2013, p. 80-89 (www.cairn.info/revue-politique-etrangere-2013-3-page-80.htm).
- JEANGÈNE VILMER Jean-Baptiste, « Quand la France armera ses drones », *L'Armée de l'air : se transformer pour préparer l'avenir (Les Cahiers de la Revue Défense Nationale, spécial Salon du Bourget 2015)*, p. 101-106 (www.cairn.info/revue-politique-etrangere-2013-3-page-80.htm).
- JOIGNOT Frédéric, « Faut-il interdire les robots tueurs ? », *Le Monde Culture & Idées*, 17 octobre 2015 (www.lemonde.fr/culture/visuel/2015/10/17/faut-il-interdire-les-robots-tueurs-autonomes_4790497_3246.html).
- LAMBERT Dominique, « L'éthique de la robotique, l'interaction homme-machine », mai 2014 (www.unog.ch/).
- LE CORRE Benoît, « Un rite funéraire pour les robots au Japon, c'est pas si étrange », *Le Nouvel Obs*, 11 mars 2015 (<http://tempsreel.nouvelobs.com/>).
- LEBLAL Serge, « Déjà le trop plein de chabot », *Le Monde Informatique* (LMI), 10 octobre 2016 (www.lemondeinformatique.fr/actualites/lire-edito-deja-le-trop-plein-de-chabots-66177.html).
- LIN Patrick, « Relationships with Robots: Good or Bad for Humans? », *Forbes*, février 2016 (www.forbes.com/sites/patricklin/2016/02/01/relationships-with-robots-good-or-bad-for-humans/#663f79f87adc).
- MCKINSEY Quarterly, « Où les machines pourraient déjà remplacer les humains, et où elles ne le pourraient pas (encore) », *ParisTech Review*, 17 juillet 2016 (www.paristechreview.com/).
- MARCHAND Leila, « Intelligence artificielle : au Japon, un robot va remplacer 34 salariés en assurance », *Les Échos*, 3 janvier 2017 (www.lesechos.fr/).
- MILLER Marine, « Les robots ébranlent le monde des avocats », *Le Monde*, novembre 2016 (www.lemonde.fr/o21/article/2016/11/29/les-robots-ebanlent-le-monde-des-avocats_5039852_5014018.html).
- MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES (MINEFI), « Axelle Lemaire lance la stratégie nationale en intelligence artificielle », janvier 2017 (www.economie.gouv.fr/strategie-intelligence-artificielle-France-IA).
- PELLERIN Cheryl, « Human-Machine Teaming Represents Defense Technology Future », octobre 2015 (www.defense.gov/).
- QUINTANA Elizabeth (Dr.), « Air Power and Autonomy », *Penser les ailes françaises* n° 33, juillet 2015, p. 90-102 (www.cerpa.air.defense.gouv.fr/images/pdf/Plaf/Plaf_33.pdf).
- « Retour vers le futur : Poutine a déclaré l'ère des robots militaires » [en russe], *Rambler.ru*, janvier 2017 (<https://news.rambler.ru/politics/35932393-nazad-v-budushee-putin-obyavil-eru-boevyh-robotov/>).

Robots et intelligence artificielle : quelle place pour l'homme dans les futures capacités militaires françaises ?

ROSENBERG Matthew et MARKOFF John, « The Pentagon's 'Terminator Conundrum': Robots That Could Kill on Their Own », *The New York Times*, 25 octobre 2016 (www.nytimes.com/2016/10/26/us/pentagon-artificial-intelligence-terminator.html).

ROTHMAN Wilson, « Unmanned Warbots of WWI and WWII », *Gizmodo*, 24 mars 2009 (<http://gizmodo.com/5181576/unmanned-warbots-of-wwi-and-wwii>).

RUFFO Marie-des-Neiges, « Le robot, étranger de l'éthique » (conférence), 21 mai 2013 (www.ed1.ulg.ac.be/sd/textes/20130521-Ruffo.pdf).

RUSSEL Stuart, « Robotics: Ethics of artificial intelligence », *Nature* n° 521, 27 mai 2015, p. 415-418 (www.nature.com/news/robotics-ethics-of-artificial-intelligence-1.17611).

RUSSELL Stuart, « Robots in war: the next weapon of mass destruction ? », *World Economic Forum*, 17 janvier 2016 (www.weforum.org/agenda/2016/01/robots-in-war-the-next-weapons-of-mass-destruction/).

SCALES Robert H. (Major General), « Urban Warfare: A Soldier's View », *Military Review*, janvier-février 2005, p. 9-18 (www.au.af.mil/au/awc/awcgate/milreview/scales.pdf).

« Les États-Unis veulent accélérer l'arrivée des voitures autonomes », *Sciences & Avenir*, 20 septembre 2016 (www.sciencesetavenir.fr/).

SHEAD Sam, « Investors are backing more AI startups than ever before », *World Economic Forum*, 26 juin 2016 (www.weforum.org/agenda/2016/06/investors-are-backing-more-AI-startups-than-ever-before).

STAMP Jimmy, « Unmanned Drones Have Been Around Since World War I », *Smithsonian.com*, 12 février 2013 (www.smithsonianmag.com/arts-culture/unmanned-drones-have-been-around-since-world-war-i-16055939/).

THEILLIER Damien, « Arendt versus Eichmann : la banalité du mal », *Contrepoints*, 29 mai 2013 (www.contrepoints.org/2013/05/29/125917-arendt-versus-eichmann-la-banalite-du-mal).

TISSERON Antonin, « Robotique et guerres futures : les armées de terre face aux évolutions technologiques », *Cahiers de l'Irsem* n° 12, 2012, 42 pages (www.defense.gouv.fr/content/download/170699/1841442/file/Cahier%2012%20-%202012.pdf).

WORK Bob, discours du secrétaire d'État adjoint à la Défense devant le *Reagan Defense Forum*, 7 novembre 2015 (www.defense.gov/News/Speeches/Speech-View/Article/628246/reagan-defense-forum-the-third-offset-strategy).

ZELLER Tristan, « Les robots militaires sont là... et maintenant ? », *Pensée mili-terre* (CDEC), 2015 (www.penseemiliterre.fr/les-robots-militaires-sont-la-et-maintenant-_2015584.html).

Entretiens

- M. Rodolphe GÉLIN, directeur de recherche et responsable des projets collaboratifs, SoftBank Robotics (ex-Aldebaran), novembre 2016.
- Jérôme DE LESPINOIS, chargé d'études à l'Institut de recherche stratégique de l'école militaire (Irsem), mars 2017.
- M. Antoine PETIT, président-directeur-général de l'Institut national de recherche en informatique et en automatique (Inria), mars 2017.
- Jean-Christophe PITARD-BOUET, chef de la division études et développements au Centre études, réserves et partenariats de l'Armée de l'air, mars 2017.
- M^{me} Marie-Véronique SERFATY, responsable du domaine scientifique ingénierie de l'information et robotique, direction générale de l'armement, mars 2017.

Principaux enjeux des objets connectés pour la défense, *et le Verbe s'est fait chair*

Frédéric BARBRY

| Colonel (terre), auditeur de la 66^e session du CHEMA.

État de l'art

Des objets connectés, focus particulier...

Un objet connecté peut être défini comme une entité physique dotée d'une interface lui permettant de délivrer des informations. Ce dispositif peut être statique (délivrance d'une donnée unique et pérenne ⁽¹⁾) ou dynamique (mesure d'une donnée variable, comme un thermomètre par exemple). Schématiquement, le processus de fonctionnement d'un objet connecté peut être résumé en 3 phases : extraction/agrégation des données, analyse et action cognitive. La première phase exige un minimum de fiabilité dans le recueil et la transmission de la donnée. En effet, l'adage « *garbage in, garbage out* » ⁽²⁾ se trouve démultiplié par l'introduction de données erronées. Pour autant, la deuxième phase d'analyse peut pallier cette lacune par abduction ⁽³⁾, dans la mesure où le phénomène de corruption des données n'est pas endémique. Enfin, il convient de noter que la dernière phase constitue la réelle plus-value de l'*Internet* des objets (IdO) avec une action qui traduit un « *so what* » du recueil massif d'informations.

Le système de transmission diffère selon les usages. Il existe à ce jour plus d'une vingtaine de protocoles différents qui assurent l'échange des données entre l'objet connecté et son terminal. Très schématiquement, c'est la nature de l'usage qui détermine le choix du mode de transmission ⁽⁴⁾. En effet, les objets connectés n'ont pas tous les mêmes impératifs en termes de coût, temps de latence, débit d'émission, autonomie, distance du signal. Ainsi, si un thermomètre connecté domestique peut être branché sur le secteur et bénéficier de la *box* de son propriétaire à proximité, il en va différemment d'un capteur sismique déposé en milieu désertique.

(1) Cas d'un objet doté d'une puce *RFID* (*Radio Frequency Identification*), avatar numérique et connecté du code-barres.

(2) « Mauvais à l'entrée, mauvais à la sortie ».

(3) En science cognitive, l'abduction est une forme de raisonnement intuitif qui consiste à supprimer les solutions improbables. Cette notion s'oppose à une logique d'exploration systématique.

(4) Les réseaux et les technologies radios s'affrontent dans une concurrence acharnée (réseau Sigfox, protocole LoRaWAN, les technologies Bluetooth 4.0 ou DASH7...). Ils proposent une réponse très efficace et fiable aux besoins spécifiques de communication des objets connectés grâce à un remarquable compromis débit/portée et avec d'excellentes performances de gestion d'énergie.

Les objets connectés envahissent notre quotidien. Ils semblent par bien des aspects révolutionnaires mais ils ne sont que la traduction domestique de systèmes plus anciens et éprouvés, les machines à machines ou *M2M* ⁽⁵⁾, à usage plus industriels et cantonnés dans des sphères plus restreintes. Aujourd'hui, l'essor des objets connectés est rendu possible par la miniaturisation des composants, la faiblesse des coûts et la disponibilité des réseaux. En effet, quand ils ne sont pas cantonnés à la maison, ils bénéficient d'une liaison nomade *via* les smartphones ⁽⁶⁾ (majoritairement) ou *via* des protocoles dédiés (cf. note de bas de page n° 3). La totalité des objets peut être connectée, selon différents processus (de manière native ou par extension). On estime qu'à ce jour moins de 1 % des objets sont connectés.

Tous les secteurs sont concernés par cette révolution. Si le segment automobile semble l'un des plus avancés (voiture autonome, entretien prédictif, pneus intelligents...), c'est, de manière moins intuitive, le monde agricole ⁽⁷⁾ qui possède un taux de pénétration parmi les plus importants. En effet, plus de 60 % des exploitants possèdent d'ores et déjà des objets connectés. Ceux-ci leur permettent d'optimiser la production (drone de surveillance des parcelles, tracteurs, mangeoires intelligentes, caméra automatique d'aide au vêlage...). Selon une enquête, ce taux devrait même avoisiner les 80 % dans les deux prochaines années. De fait, aucun segment d'activité n'échappe à la voracité de ce marché émergent : loisirs, santé, éducation, commerce, domotique, alimentation, surveillance...

...à l'Internet des Objets (IdO), panorama général

Aujourd'hui, on estime à 7 milliards le nombre d'objets connectés dans le monde. Les prévisions de croissance sont exponentielles et ils devraient être environ 25 Mds en 2018 pour doubler et atteindre 50 Mds à l'horizon 2020. L'IdO désigne donc la nébuleuse de ces objets connectés, que l'Union internationale des télécommunications (UIT) caractérise comme « l'infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets grâce aux technologies de l'information de la communication interopérables existantes ou en évolution ».

Au niveau mondial, l'impact économique potentiel de l'IdO devrait représenter l'équivalent de 11 % de l'économie globale ⁽⁸⁾. Rien qu'en France, les dépenses pour l'IdO sont estimées à 118 Mds d'euros pour 2018, avec une progression de 245 % en 5 ans ⁽⁹⁾. Il n'est donc pas étonnant que cet Eldorado économique voit d'un mauvais œil les cassandres environnementales ⁽¹⁰⁾ s'inquiéter de la surexposition des populations aux ondes issues de la multiplication des objets connectés. Les ondes électromagnétiques

(5) *M2M* est l'association des TIC avec des objets dits intelligents/communicants dans le but de fournir à ces deniers les moyens d'interagir sans intervention humaine avec le système d'information.

(6) Nombre de *smartphones* dans le monde, sans oublier l'Afrique avec un taux de pénétration (350 millions d'unités en 2017) qui témoigne d'une croissance significative (40 % de 2013 à 2015).

(7) Données pour la France, d'après objetconnecte.com, septembre 2016.

(8) MCKINSEY GLOBAL INSTITUTE, juin 2015.

(9) Source : IDC, novembre 2014.

(10) L'association « Robin des toits » en étant l'expression la plus emblématique, pour la France (www.robindestoits.org/).

émises par les téléphones portables, les tablettes ou autres objets connectés sont en effet potentiellement dangereuses pour les enfants en bas âge ⁽¹¹⁾, selon un rapport publié en juillet 2016 par l'Agence nationale de sécurité sanitaire.

L'IdO est ainsi considéré comme la troisième phase d'évolution majeure d'*Internet* « *Web 3.0* » qui fait suite à l'ère du « *Web 2.0* » ou « *Web-Social* » avec notamment l'explosion des réseaux sociaux. L'IdO figurant comme l'extension d'*Internet* aux objets du monde réel, il en constitue la matérialisation physique. Ainsi, pour reprendre l'exemple de la voiture connectée, la plus-value ne réside pas dans le diagnostic de la panne éventuelle mais dans le processus induit : intégrité de la voiture → localisation du véhicule → disponibilité de la pièce défectueuse → acheminement si valeur d'usage du véhicule supérieure → etc.

On est ainsi passé de la virtualité de données évanescentes à la réalité physique d'objet du quotidien : *et le verbe s'est fait chair*.

Un écosystème encore en gestation

À ce stade de la montée en gamme des objets connectés, de nombreux domaines sont encore en phase de stabilisation. Trois d'entre eux méritent une attention toute particulière : la sécurité informatique, la souveraineté et les aspects juridiques.

La cybersécurité liée aux objets connectés apparaît comme l'axe majeur et structurant devant encadrer l'essor de l'IdO. Selon une dernière étude parue, plus de 80 % des objets connectés actuellement sur le marché présenteraient des failles de sécurité. Si la responsabilité du consommateur ne peut pas être totalement exclue ⁽¹²⁾, il n'en demeure pas moins que les constructeurs n'ont pas pris la pleine mesure des enjeux : absence de mise à jour des *firmwares* ⁽¹³⁾, mot de passe générique, obsolescence native des mesures de protection. Ainsi, les objets connectés constituent désormais la principale bête noire des Directeurs des services informatique (DSI) en œuvrant comme autant de cheval de Troie dans un système de systèmes de plus en plus interconnectés. On se remémorera sans peine cette attaque par déni d'accès d'un grand groupe industriel par l'utilisation malveillante... de réfrigérateurs connectés !

Ces attaques sont pourtant relativement simples et ne font qu'étendre aux objets connectés des pratiques en œuvre depuis les années 1990. Aujourd'hui, les menaces sont encore plus élaborées compte tenu justement de l'interdépendance issue de l'IdO. En octobre 2016, une équipe de chercheurs internationaux ⁽¹⁴⁾ a montré que le piratage des outils de fabrication additive pouvait avoir des conséquences très concrètes, dans le monde réel. En l'occurrence, il s'agissait de s'attaquer à l'ordinateur de contrôle de l'imprimante 3D qui fabrique les hélices de drone, en y introduisant des

(11) Selon les experts, les enfants – et notamment *in utero* – sont les plus sensibles aux ondes électromagnétiques, car leur cerveau est en cours de transformation.

(12) Les utilisateurs rechignent à modifier le mot de passe par défaut, omettent d'activer le cryptage des données, n'assurent pas les mises à jour recommandées...

(13) Micro-logiciel qui constitue le « cerveau » de l'entité informatique considérée.

(14) Université Ben Gourion du Negev, *Singapore University of Technology and Design (SUTD)* et *University of South en Alabama*.

défauts invisibles à l'œil nu. Le résultat est sans appel. L'hélice est imprimée avec son défaut caché, qui, après quelques minutes de vol, provoque la chute et la destruction du drone...⁽¹⁵⁾

La question de la souveraineté demeure intrinsèquement liée à l'IdO. En effet, la puissance publique a déjà été mise en échec face au fait *Internet*. Le réseau, par nature dématérialisé et transfrontalier, s'adapte mal à l'application des droits nationaux. Par ailleurs, une gouvernance mondiale s'avère d'autant plus compliquée à mettre en place qu'elle se heurte à l'absence de consensus sur la nature même d'*Internet*, espace de liberté absolue ou simple extension du périmètre étatique. C'est une des raisons principales qui a prévalu aux échecs successifs de l'ONU lors des forums de Genève (2003) et Tunis (2005), portant sur la société de l'information.

Il convient également de conserver à l'esprit la bataille de haute lutte remportée – contre le reste du monde – par le vice-président Al-Gore en 1997 lorsque l'administration Clinton s'était emparée de l'*Internet Corporation for Assigned Names and Number (ICANN)*. Cette situation dominante des États-Unis sur la gouvernance d'*Internet* constitue un abus manifeste qu'il convient de ne pas reproduire. L'Union européenne doit peser de tout son poids diplomatique sur la scène internationale afin que l'IdO, amplifiant le phénomène avec l'accroissement exponentiel des données générées, ne soit pas une fois encore la proie de nos alliés américains⁽¹⁶⁾. La question de l'hébergement des flux acquiert en effet une importance d'autant plus grande que la valeur⁽¹⁷⁾ qui leur est intrinsèquement liée pourrait ainsi échapper aux producteurs.

Dans une société occidentale marquée au fer rouge par la judiciarisation des interactions sociales, les objets connectés soulèvent de nouvelles problématiques. Dans l'hypothèse de la survenue d'un accident ou incident causé par un objet connecté, la responsabilité devra être déterminée à l'aune du droit national. En France, la suspicion de responsabilité est conférée au propriétaire⁽¹⁸⁾ du bien qui a causé le tort. Pour autant, sans constatation de « défaut d'usage » du bien, il sera intéressant de noter la jurisprudence à venir. Dans tous les cas, ce pan juridique mérite une anticipation d'autant plus urgente que les dispositifs autonomes vont prendre une importance considérable dans les années à venir (voitures autonomes, régulation du trafic, dispositifs aériens de livraison...).

Des applications militaires à consolider

Smart Soldier

La défense s'est investie très rapidement dans l'utilisation d'objets connectés à des fins opérationnelles. Le vocable a d'ailleurs évolué et les **systèmes d'armes** ont cédé

(15) Bulletin Innovation et ruptures technologiques de défense (US, UK, DE) n° 5 du 30 novembre 2016.

(16) Sans même évoquer les systèmes d'espionnage *PRISM* et *Echelon*, il convient de garder à l'esprit que Google représente 95 % des recherches mondiales et demeure en capacité d'exercer – outre son influence – un droit de vie ou de mort sur la majorité des sites référencés.

(17) On parle de « nouvel or noir ».

(18) Article 1384 alinéa 1^{er} du code civil.

le pas aux **systèmes de systèmes**. En effet, les plateformes de combat deviennent de plus en plus connectées, au sein d'un maillage cohérent. Pour autant, d'une position de précurseur, les armées ont marqué le pas, notamment pour des problématiques de transmission et de sécurisation des données. Dans cet environnement digitalisé, les entités constitutives du système des systèmes deviennent autant de multicapteurs du champ de bataille. Dans cette course à la connectivité, les Américains ⁽¹⁹⁾ et les Israéliens possèdent une longueur d'avance sur les autres armées occidentales. Bien plus précocement que pour le Vieux Continent, ces deux armées ont su très rapidement anticiper sur les opportunités que pouvaient apporter les objets connectés ⁽²⁰⁾ pour les militaires.

Si beaucoup d'objets connectés militaires apparaissent davantage comme l'extension naturelle des systèmes d'armes déjà en place, c'est le secteur médical qui tire pleinement le secteur en exploitant au mieux les capacités nouvelles. À l'instar des systèmes personnels qui équipent d'ores et déjà de nombreux sportifs ou personnes soucieuses de leur santé ⁽²¹⁾, l'armée israélienne a mis au point un bracelet électronique connecté qui permet une remontée en temps réel des « constantes » ⁽²²⁾ des soldats qui en sont dotés. Ces différentes mesures, corrélées avec les données issues de leur dossier médical permettent un suivi en temps réel du potentiel physiologique des militaires. On imagine ainsi le gain de temps réalisé par les équipes médicales pour le tri des blessés après un contact avec l'ennemi ou bien encore pour le chef de mission afin de mieux appréhender le stress de sa troupe. Ici encore, il est patent de constater la nécessité de disposer de dispositifs sécurisés, fiables et dont le traitement demeure dans un périmètre de confiance. Il est à noter que la France est précurseur dans le domaine, au sein de l'UE, en étant la seule Nation à offrir une base juridique, sécurisée ⁽²³⁾ et déontologique au Dossier médical du patient (DMP).

Smart Base

À une plus vaste échelle, les objets connectés trouvent naturellement leur place dans les quartiers militaires, qu'il s'agisse de petites emprises ou de plus vastes périmètres comme des ports ou des bases aériennes ⁽²⁴⁾. Dès lors, ces espaces fonctionnent comme des *Smart Cities*. Certes, de timides percées ont été réalisées dans l'implémentation de ces nouvelles technologies. L'effort le plus emblématique demeure l'optimisation de la logistique avec la mise en place de puces *RFID* sur les unités de base (pièces ou lots de rechanges, colis, container...) couplés à un système d'information logistique

(19) 9 Mds de \$ ont été injectés par le gouvernement fédéral en crédit de recherche pour le seul segment de l'IdO

(20) Technologie duale par excellence.

(21) Marché en pleine expansion du *quantified self*.

(22) Tension, rythme cardiaque, concentration d'oxygène dans le sang, volume d'air inspiré...

(23) Les hébergeurs de DMP doivent obtenir l'autorisation des autorités administratives et certifier l'atteinte de la norme ISO 27005.

(24) En juin 2015, sur la base aérienne 105 d'Évreux, le chef d'État-major de l'Armée de l'air a présenté le concept *Smart Base*. Il s'inscrit dans la dynamique du développement des *Smart Cities* et tend à ouvrir la base afin d'optimiser son potentiel, notamment *via* des partenariats innovants. Il s'agit d'un projet pilote qui devrait – à terme – irriguer toutes les Bases de défenses (BdD).

performant. Pour autant, des pistes nouvelles demeurent à explorer dans le but tant de réduire les coûts que de gagner en confort dans l'exécution des tâches quotidiennes.

Dans le cadre de la collecte des ordures, il est envisageable de placer des capteurs sur les containers de déchets afin de mesurer le taux de remplissage, l'ensemble étant couplé avec le planning d'activité de la base afin de contractualiser au mieux le ramassage des ordures d'après une estimation prédictive constatée. Sur un principe identique, la confection des repas pourrait davantage s'appuyer sur une analyse multicritère déclenchée par un indicateur de présence (badge connecté). De la même façon, la technologie autorise désormais l'analyse plus fine des flux vidéo. Il est ainsi envisageable de déterminer les flux récursifs des mouvements routiers sur une base pour moduler les zones d'éclairage en fonction des besoins réels et non pas estimés. Les mêmes technologies peuvent être appliquées aux fonctions protection et sauvegarde.

Les exemples peuvent se décliner à l'infini. Des villes ou des quartiers qui ont d'ores et déjà adopté ce fonctionnement⁽²⁵⁾ (en France comme à l'étranger) pourraient servir de modèle à nos emprises militaires. Le coût d'investissement n'est pas négligeable mais il est à mettre en relation avec les économies d'échelle escomptées, soit en gains directs par économie financière, soit en bénéfice induit avec la dynamisation de tout un écosystème vertueux⁽²⁶⁾.

Smart Battle Field

Pour les cinéphiles adeptes des problématiques de renseignement, ils n'auront pas manqué de regarder le film *Snowden*, ou la série *Le bureau des légendes*. Ces deux œuvres fixent avec beaucoup de réalisme les nouvelles méthodes qui sont désormais accessibles avec l'interconnexion des bases de données, la perméabilité des réseaux et les faiblesses sécuritaires. Le champ des possibles étant infini avec l'émergence de l'IdO, seules les Opex (Opérations extérieures) seront évoquées dans ce paragraphe, dans l'acception d'un théâtre d'opération de type *Barkhane* ou centre-Europe.

Quand on évoque les objets connectés du champ de bataille, on pense bien évidemment à la bulle info-valorisée. Les différents systèmes d'armes modernes agissent comme autant d'objets connectés qui interagissent entre eux en remontant les données issues de leurs capteurs afin qu'ils soient agrégés à l'échelon supérieur. Il s'agit d'un système fermé pour lequel les ponts avec le réseau *Internet* civil sont strictement limités et surveillés. Dans les faits, il s'agit essentiellement d'éléments et actes de maintenance télé-opérés par des industriels⁽²⁷⁾ agréés. Dans le cas présent, les armées, du fait des volumes d'objets connectés engagés, sont encore au balbutiement de l'IdO du champ de bataille. C'est précisément la raison pour laquelle il convient de mettre en place un « *cloud* » militaire⁽²⁸⁾, qui intègre les contraintes spécifiques, comme les conditions

(25) *Smart-grid* notamment qui consiste à gérer les flux énergétique en fonction du besoin réel.

(26) Maintien du savoir-faire industriel des PME/PMI, innovation, emplois indirects, compétitivité à l'international, imposition des normes de fait, vitrine technologique....

(27) Dans le domaine aéronautique, mais bientôt également pour les modules terrestres avec *Scorpion*.

(28) Sur le modèle des clouds privés qui sont en service dans le monde civil. L'*US Army* y a d'ores et déjà adhéré avec le programme *US Army Private Cloud Contract (APC2)*. Ce contrat prévoit la livraison sur les théâtres d'opération de *data centers* mobiles.

dégradées ou des dénis d'accès au réseau. Les unités doivent en effet pouvoir manœuvrer dans des configurations de connectivité très variées (connectée, déconnectée, intermittente...), nécessitant des serveurs de réplication asynchrone, une redondance des relais, le recours au satellite... Ce *cloud* privé devra être éprouvé pour répondre aux contraintes spécifiques de la défense, selon une analyse des risques multicritères qui repose sur quatre items : disponibilité, confidentialité, intégrité et traçabilité.

En conséquence dès demain, du fait des dispositifs connectés portables qui doteront en masse les combattants, mais aussi en raison de la masse informationnelle environnante ou bien encore de la saturation du champ de bataille par des capteurs connectés (29), les armées entreront dans un nouvel espace de conflictualité où la gestion et la ségrégation des données utiles deviendront un des facteurs clé de la victoire. À cette fin, il conviendra de maîtriser la sécurité de bout en bout des données, que ce soit au travers de la cryptographie ou par l'implémentation de certificats. Parallèlement, un autre défi à relever sera celui des transmissions en adoptant des standards qui puissent être interopérables dans le cadre de coalitions avec nos alliés et partenaires.

Sans que cela puisse paraître pour une caution verte ou clause de bonne conscience écocitoyenne, les aspects environnementaux devront être pris en compte. D'une part, il s'agira de bien dimensionner les besoins réels en équipement dans la mesure où les objets connectés, civils et militaires, sont particulièrement énergivores en ressources, dites terres rares (30). D'autre part, il conviendra de ne pas disséminer de manière irrémédiable dans la nature des dispositifs qui comportent des substances dangereuses pour l'environnement.

Enfin, il conviendra de mettre en place des solutions de stockage de données afin de faire face à l'afflux sans commune mesure avec ce qui existe actuellement. Des solutions techniques existent d'ores et déjà dans le monde civil pour répondre à ce besoin nouveau. Compte tenu des impératifs de temps de latence (impératif de réactivité), ces *data centers* devront être positionnés au plus près du centre de gravité des opérations. Une fois en place, des supercalculateurs pourront prendre le relais afin d'assurer le traitement de la masse d'informations.

Un potentiel infini encore sous-exploité

Gagner la bataille de « l'infobésité »

L'infobésité désigne la surabondance d'informations générée par la multitude de données qui nous parviennent en permanence en raison de la multiplication des capteurs et des systèmes numériques. Avec l'accroissement exponentiel de ces derniers, on estime que 90 % des données disponibles dans le monde ont été générées dans les deux dernières années. Le volume de données mondiales passera ainsi de 4,4 Zettabytes

(29) Que ce soit par des capteurs statiques ou dynamiques, voir à cette fin l'article d'Emmanuel CHIVA sur ce système de drones *Perdrix* : « Un essaim de 103 drones aériens démontre des capacités de coordination », *VMF 214 – le blog*, 17 janvier 2017 (<https://vmf214.net/2017/01/17/un-essaim-de-103-drones-aeriens-demontre-des-capacites-de-coordination/>).

(30) Ces 17 métaux aux propriétés proches sont, contrairement à leur nom, plutôt répandus mais à des concentrations souvent faibles et mélangés avec d'autres métaux, ce qui complique leur exploitation.

(Zo⁽³¹⁾) en 2013 à 44 Zo en 2020⁽³²⁾. Dans les prochaines années, le volume mondial de données doublera tous les 18 mois. Plus important, sur la totalité des données produites en 2013, 65 % l'ont été par les consommateurs alors qu'avant 2010, la courbe était inversée avec la prédominance du secteur industriel. Aujourd'hui, les réseaux sociaux prennent une place considérable dans la génération des données. Quand Twitter produit quotidiennement 7 To de données, Facebook en génère 10. En 2020, la part des objets connectés devrait être majoritaire dans la production des données.

Cette augmentation inéluctable des données induit la création de « *data center* » de plus en plus performant. Et c'est ici que l'enjeu environnemental vire au paradoxe. Sous la double contrainte du changement climatique et de l'épuisement des ressources naturelles, les innovations portées par les TIC devraient pouvoir s'inscrire dans une dynamique de développement durable. Et on aurait pu imaginer que les gains d'énergies induits par des systèmes intelligents feraient pencher la balance en faveur de la digitalisation croissante. Il n'en est rien. Actuellement, les TIC représentent 10 % de la consommation d'énergie et 2 % des émissions de CO₂ mondiales. D'ici 2020, émissions et consommation d'énergie en lien avec les TIC dépasseront celles de tous les autres secteurs. Les serveurs, dont le fonctionnement exige des systèmes de climatisation en continu, sont particulièrement énergivores. Les quelques 500 000 centres de données existants⁽³³⁾ dans le monde consommeraient environ 30 Mds de watts d'électricité par an, soit l'équivalent de la production de 30 centrales nucléaires. Certes, des tentatives sont en cours pour diminuer cette déperdition colossale. Pour autant, le fléau de la balance énergétique penche encore actuellement, et pour quelques décennies, du mauvais côté.

Cette assertion énergétique s'avère fondamentale pour la défense. En effet, si la consommation induite par les cinq *data centers* principaux localisés en métropole relève d'une problématique maîtrisée, il en va tout autrement sur les théâtres d'opération ou la génération d'énergie constitue un souci constant.

Les défis du Big Data⁽³⁴⁾

Par opposition au *Big Data*, on parle quelque fois de « *Small Data* », des données dont la volumétrie et les formats les rendent compréhensibles et utilisables par le commun des mortels. Un aphorisme résume l'idée que « le *Big Data* est taillé pour les machines, le *Small Data* est taillé pour les hommes ».

Pour faire face à l'avalanche des données, les technologies du *Big Data* sont les seules à même de pouvoir traiter et exploiter cet océan de données dans le but d'en tirer des informations intelligibles et pertinentes. Le *Big Data* est caractérisé par la règle des

(31) Un Zo = 10²¹ octets ; PM un Yo = 10²⁴ octets, un Eo = 10¹⁸ octets, un Po = 10¹⁵ octets, un To = 10¹² octets...

(32) Thierry BERTHIER (maître de conférence en mathématiques à l'Université de Limoges), « Sur la valeur d'une donnée », mai 2014, Article n° IV.3, Chaire de Cyberdéfense et Cybersécurité.

(33) Et dont la répartition géographique s'établit comme suit : Asie-Pacifique 40 %, Amérique du Nord 34 % et Europe Middle East Africa 22 %.

(34) En France, la Commission générale de terminologie et de néologie (en lien avec l'Académie française) a statué en 2014 que l'expression anglaise « *Big Data* » se traduisait officiellement par « Megadonnées ».

« 6V » : le Volume, la Variété, la Vitesse (ou Velocité), la Volatilité ⁽³⁵⁾, la Véracité et la Validité. Bien qu'il n'y ait pas de définition précise du volume minimum du *Big Data*, le terme est souvent utilisé lorsque l'on dépasse le millier de To, des volumes qui posent de nouveaux défis d'intégration et de traitement.

Au final, « *Big is not bigger ; Big is different* ». Autrement dit, le changement d'échelle n'implique pas les mêmes outils en plus puissants, mais d'autres outils, du fait même que le changement d'échelle fait aussi totalement changer la logique sous-jacente. Le *Big Data* n'appelle donc pas des bases de données plus importantes ou des disques durs plus gros, mais des technologies singulières.

Une fois la matière (données) et les outils (gestion du *Big Data*) en place, il convient d'appliquer la recette (algorithme) afin d'élaborer un produit fini. L'algorithme est la clé de voute du système dans la mesure où c'est lui qui va permettre d'extraire depuis des données utiles un résultat cohérent sous forme d'un absolu, d'une tendance ou d'une prédiction. À ce stade, il ne faut pas oublier que l'algorithme n'est que la traduction en langage codé d'une vision humaine, imparfaite et faillible fondée peu ou prou sur une résultante de calculs de probabilités. C'est la raison pour laquelle les systèmes sont désormais renforcés dans leurs capacités, notamment *via* le *deep learning*. Ce système d'auto-apprentissage et de classification, basé sur des « réseaux de neurones artificiels » numériques, est d'ores et déjà utilisé par les géants du GAFÀ ⁽³⁶⁾ dans leur quête d'intelligence artificielle. Concrètement, le *deep learning* permet donc à un programme de comprendre des défis complexes ⁽³⁷⁾.

Les recherches en la matière sont très prometteuses mais non dénuées de risques. Dans une logique purement commerciale, on comprend bien que la recherche de maximisation de gains représente un impératif, voire un dogme intangible. Il en est tout autrement pour les applications militaires, notamment pour les systèmes d'information opérationnelles et de commandement. Une bataille ne se remporte pas à tout prix et l'anéantissement de l'ennemi ne constitue aucunement un invariant de l'état final recherché. C'est en substance ce que viennent de modéliser les chercheurs de la Google's DeepMind Division, en mettant en évidence qu'un système numérique de type neuronal, entraîné à apprendre « par expérience » pour poursuivre une stratégie de conquête efficiente ⁽³⁸⁾, devenait hautement agressif en phase de compétition. Cette tendance « logique » peut cependant être atténuée par des systèmes de valorisation de « mode collaboratif » et non « destructif ».

Il convient donc d'envisager au plus tôt l'intégration des aspects éthiques et philosophiques au sein des outils à naître. Cette réflexion ne doit pas seulement envisager les risques qu'ils pourraient faire courir aux humains. Elle doit aussi prendre en compte les dangers que les humains pourraient se faire courir à eux-mêmes par une appréciation erronée de ce que ces machines peuvent leur apporter, autrement dit de

(35) Il s'agit de la « durée de vie » des données générées, autrement dit, pendant combien de temps elles sont valides.

(36) Google – Apple – Facebook – Amazon.

(37) Langage parlé, interprétation d'images complexes...

(38) Jeux coopératif entre robots neuronaux dans la quête de pommes.

ce qu'elles sont réellement, au-delà des fantasmes. À défaut, il existe un risque de déshumanisation⁽³⁹⁾ de l'art de la guerre : une perte de cette âme qui constitue à la fois un garde-fou et la crédibilité de nos armées.

Le commandement prédictif, atout maître vs désincarnation du combat futur ?

Finalement, les objets connectés, et par eux l'*Internet* des objets, ne sont qu'un outil, la première couche (primitive mais indispensable) d'un système plus complexe et dont la force réside dans la capacité d'agrégation, voire de compréhension d'un monde environnant de plus en plus difficile à cerner⁽⁴⁰⁾. L'IdO présente toutes les caractéristiques d'une technologie de rupture. Elle vient en effet découpler le champ des possibles que ce soit sur les différents théâtres d'opérations comme au quartier. Alors même que la tendance actuelle tendait à suivre la fameuse loi d'Augustine, l'IdO vient redonner à la masse critique et à la saturation toutes ses lettres de noblesse.

« *In the year 2054, the entire defense budget will purchase just one tactical aircraft. This aircraft will have to be shared by the Air Force and Navy 3½ days each per week except for leap year, when it will be made available to the Marines for the extra day.* » (Norman Ralph AUGUSTINE, *Augustine's Laws*, 1984).

De par cette omniprésence de l'IdO (qui prend toutes les formes de l'ubiquité), grâce au traitement de plus en plus fin du *Big Data* généré (omniscience), il devient tout à fait envisageable d'implémenter dans les SIOC (Systèmes d'information opérationnel et de commandement) futurs une notion de prédictabilité. Ce nouvel outil d'aide au commandement constituera une véritable révolution dans la conduite des opérations. On peut ainsi aisément envisager de réduire l'empreinte au sol des états-majors de type opératifs et stratégiques en supprimant une large part de la ressource humaine. À titre d'illustration, tous les aspects liés au *reporting* ainsi qu'à l'analyse de l'ennemi pour le J2 pourraient être produits par le système, sur la base de la remontée d'informations des objets connectés disséminés sur le terrain. La plus-value du J2 (faire vivre l'ennemi) serait assurée également par le système, en croisant en temps réel son état de connaissance issu du *deep learning*, enrichi des dernières données disponibles sur *Internet*⁽⁴¹⁾.

Il ne s'agit en aucun cas d'un scénario de science-fiction. Les solutions techniques existent. Il convient cependant de les durcir (cybersécurité des objets connectés), d'assurer les transmissions (débits, élongations, standards, interopérabilité), de mettre en place les solutions de *data center* déportées ainsi que le noyau logiciel adéquat. Il y a quelques années encore, le fait de battre un joueur d'échec semblait hors de portée pour un ordinateur⁽⁴²⁾. Aujourd'hui, plus un seul être humain ne saurait rivaliser avec la machine. Certes, les échecs apparaissent comme un univers fini et maîtrisable,

(39) Voire, dans le cas d'un emballement, comprendre « déshumaniser » par « retirer physiquement l'humain » de la surface de la terre.

(40) Les Anglo-Saxons le décrivent sous l'acronyme *VUCA* (*Volatility, Uncertainty, Complexity et Ambiguity*), notion introduite par l'*US Army War College*.

(41) Actualisation d'un compte Facebook, envoi d'une revendication par Twitter...

(42) Le 11 mai 1997, l'ordinateur *Deep Blue* a battu Garry Kasparov aux échecs (10¹²⁸ positions possibles). À cette date, les informaticiens estimaient qu'il faudrait 50 ans pour battre un humain au jeu de Go (10¹⁷² positions possibles). Mais c'est dès janvier 2016 que le programme *AlphaGo* a écrasé le meilleur joueur du monde...

au contraire du brouillard généré par la guerre. Pourtant, on pressent bien que l'intelligence humaine a atteint des limites structurelles que ne connaissent pas encore les ordinateurs. Ainsi, il ne s'agit pas de savoir si un système numérique dépassera un jour les capacités de tous les stratèges militaires mais quand.

Au-delà du seuil technologique des systèmes de systèmes doués de capacités prédictives, le chef militaire ne pourra plus penser les systèmes d'armes seulement comme des systèmes d'armes, parce qu'ils vont échapper en partie à son contrôle pour passer sous celui des concepteurs (industriels, programmeurs...). C'est le sens de la révolution des algorithmes. Or, psychologiquement, l'homme a besoin de croire que les machines autonomes ont une conscience ; c'est-à-dire une volonté et un libre arbitre. Il veut pouvoir penser qu'il peut les apprivoiser, car il s'agit de contrecarrer la vision d'une application strictement arithmétique de l'art de la guerre, sans état d'âme, ni pitié, ni empathie. Ainsi, par ce biais de la conscience numérique, l'homme – le chef militaire – entend ré-humaniser l'univers digital placé aujourd'hui sous le signe d'une froideur absolue. Les imaginer avoir ce supplément d'âme permet même de penser pouvoir les influencer, en dépit d'une programmation hermétique. Pour autant, à un horizon visible, il convient de combattre cette chimère, car il ne faut pas se tromper sur sa cause. Le fantasme d'un système « à libre arbitre » cherche à opposer au cauchemar du système sous contrôle uniquement logique une vision qui n'est pas forcément plus rassurante, mais qui rend à l'homme sa part de liberté.

Aujourd'hui, le commandant en chef d'une opération peut encore véritablement influencer sur le cours de la manœuvre. Demain, le brouillard de la guerre qui aurait dû être dissipé par les systèmes d'aide au commandement va se déporter sur le processus décisionnel. *In fine*, le chef sera placé dans une situation particulièrement inconfortable. La question philosophique réside donc dans la capacité de choix du décideur, qui aura été conseillé et appuyé par une somme d'itérations programmatiques qui dépasse l'entendement humain. Dans quelle mesure, face au vertige de l'immensité des données traitées par la machine, saura-t-il conserver son libre arbitre ?

Acronyme	Définition
APC2	<i>US Army Private Cloud Contract</i>
DASH7	nouvelle forme de transmission sans fils, utilisable dans le monde entier
DMP	Dossier médical du patient
DSI	Directeur des services informatiques
ICANN	<i>Internet Corporation for Assigned Names and Number</i>
IdO	<i>Internet des objets</i>
IoT	<i>Internet of Thing</i> , Internet des objets
ISO	<i>International Organization for Standardization</i>
LoRaWAN	<i>Long Range Wide-Area Network</i> , réseau étendu à longue portée
M2M	<i>Machine to Machine</i>
RFID	<i>Radio Frequency IDentification</i> , identification par fréquence radio
TIC	Technologies de l'information de la communication
VUCA	<i>Volatility, Uncertainty, Complexity et Ambiguity</i>

Principaux enjeux des objets connectés pour la défense, et le Verbe s'est fait chair



Graphique de maturité des objets connectés selon le cabinet Gartner, 2016.

Éléments de bibliographie

ERHEL Corinne et LA RAUDIÈRE (DE) Laure, *Les objets connectés (rapport d'information n° 4362)*, Commission des affaires économiques, Assemblée nationale, 10 janvier 2017, 147 pages (www.assemblee-nationale.fr/14/rap-info/i4362.asp).

COSQUER Christian (Général 2S) et LANCKRIET Julie, « Les objets connectés et la défense », *Les notes stratégiques*, CEIS, décembre 2015, 30 pages (www.sia-lab.fr/fr/articles/note-strategique-les-objets-connectes-et-la-defense).

GOETZ Pierre, MAUPEOU (DE) Martin et DYÈVRE Axel, « Emploi du Cloud dans les Armées : première approche des concepts et contraintes », *Les notes stratégiques*, CEIS, août 2016, 40 pages (www.sia-lab.fr/fr/articles/note-strategique-emploi-du-cloud-dans-les-armees-premiere-approche-des-concepts-et).

BABINET Gilles et VASSOYAN Robert, *Big data et objets connectés. Faire de la France un champion de la révolution numérique (rapport)*, Institut Montaigne, avril 2014 (www.institutmontaigne.org/).

FRANCE STRATÉGIE, *Demain, l'Internet des Objets, Note d'Analyse n° 22*, 12 janvier 2015 (www.strategie.gouv.fr/publications/demain-linternet-objets).

L'OBSERVATOIRE FIVES DES USINES DU FUTUR, *Cahier* (2^e édition), 2014, 112 pages (http://dk8mx37zdr9bp.cloudfront.net/corporate/PublishPaper/cahier_observatoire_2/files/docs/all.pdf).

SERGÈRE Vincent, « LoRa : LE futur réseau des objets connectés ? », *FrAndroid*, 18 octobre 2015 (www.frandroid.com/telecom/313396_lora-futur-reseau-objets-connectes).

LoRA-ALLIANCE, site officiel (www.lora-alliance.org).

SIGFOX, site officiel (www.sigfox.com/fr/).

Séminaires

- COMMISSION SUPÉRIEURE DU NUMÉRIQUE ET DES POSTES, colloque « Intelligence artificielle : des libertés individuelles à la sécurité nationale », mardi 14 février 2017.
- COMITÉ CYBERDÉFENSE DE L'ANAJ-IHEDN, conférence « Internet des objets : qui gagnera la guerre des réseaux ? », jeudi 9 mars 2017.
- CHAIRE CYBERDÉFENSE ET CYBERSÉCURITÉ SAINT-CYR, séminaire interarmées « Objets connectés et monde militaire », mardi 21 mars 2017.

Le cyberspace, nouvel espace de souveraineté à conquérir

Christophe GASANÇON

| Colonel (terre), auditeur de la 66^e session du CHEM.

Un nouveau milieu avec sa grammaire propre

Un milieu créé par sédimentation...

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le cyberspace est « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées ». Il est généralement caractérisé ⁽¹⁾ par une approche sédimentaire en trois couches.

Une **première couche « physique »** ou « **matérielle** » qui regroupe les appareils d'extrémité (ordinateurs, *box* de fournisseur d'accès *Internet*, disques durs, carte de crédit, distributeur de billet de banque...) ainsi que les infrastructures de réseau. Cet ensemble traite l'information et la transmet. Cette couche dépend d'un territoire, sur lequel sont implantés les serveurs ou fermes de données (*Datacenter*) ainsi que les câbles et les moyens de transmission terrestre, aérienne ou spatiale qui permettent leur connexion. Ce territoire a sa législation – donc sa souveraineté.

Une **deuxième couche « logique »** ou « **logicielle** » regroupe les dispositifs de codage et de programmation qu'utilisent les machines. La pensée humaine est transformée en information *via* des interfaces homme-machine et des protocoles permettant la communication entre machines au sein d'un réseau, afin qu'elles puissent se transmettre l'information.

Enfin une **troisième couche « sémantique »**, « **cognitive** » ou « **informationnelle** » regroupe les données ou métadonnées qui sont transportées par le réseau. Ces métadonnées sont qualifiées de données de masse. Elles peuvent permettre de déterminer les goûts des consommateurs et influencer ou favoriser la prise de décision d'achat. Une donnée transporte donc une information sur la personne qui la produit. Un ensemble d'informations donne un message assimilable à une opinion générale ou collective constituant la dimension informationnelle du réseau. Ainsi le cyberspace doit être appréhendé globalement au travers de cette sédimentation et non uniquement par la seule dimension logicielle.

(1) François-Bernard HUYGHE, Olivier KEMPF et Nicolas MAZZUCHI, *Gagner les Cyberconflits – Au-delà du technique*.

...qui est le support d'une nouvelle conflictualité permettant le retour de l'offensive

L'absence de facteurs déterminants comme le temps et la distance au sein du cyberspace amplifie la notion de brouillard d'une guerre numérique ou cyberguerre. Son opacité permet le retour de modes d'action directs dont les seuils d'acceptation sont plus bas que les opérations militaires conventionnelles. Il permet un retour à moindres frais de l'offensive asymétrique ou hybride, en réduisant les écarts de puissance entre les différents acteurs, voire en complément d'actions conventionnelles, tout en permettant à son auteur de se dissimuler au sein de la toile par écrans interposés. Les conflictualités dans le cyber peuvent être caractérisées par une ou plusieurs combinaisons d'actions de recherche d'informations (cyberespionnage), d'actions de perturbation, de destruction ou de prise de contrôle à distance de systèmes informatiques (cyberattaque).

Le cyber est également un milieu propice aux actions de propagande et de manipulation de l'information assimilable à de la subversion pour modifier l'opinion. En effet, la dimension informationnelle et les opinions qui y circulent sont aujourd'hui le support de mouvement de contestations, d'influence, de recrutement, voire l'objet de manipulation ⁽²⁾ où la subversion des esprits permet d'exercer la dialectique des volontés ⁽³⁾, d'affirmer ou d'imposer sa volonté sur l'autre par l'intermédiaire du « public » visé.

L'action offensive dans le cyberspace se caractérise par sa « foudroyance », ou instantanéité, en sidérant sa cible, et par son imprévisibilité en bénéficiant d'une faille ou vulnérabilité critique (« *zero-day* ») du système, inconnue du défenseur. Sa dangerosité est un facteur déterminant par la propagation parfois non maîtrisée ⁽⁴⁾ de l'arme employée mais aussi par la prolifération de l'arme elle-même ⁽⁵⁾ en d'autres armes de nature plus complexes. La cyberattaque se démarque également par son ubiquité grâce à une cible déterritorialisée pouvant être à plusieurs endroits au sein du réseau. L'indétermination ⁽⁶⁾ du début de l'attaque et sa durée favorise sa furtivité. La difficulté d'identifier son auteur avec certitude, l'attribution de l'attaque, facilite son impunité. Même si les recherches permettaient d'identifier l'adresse *IP* d'origine de l'attaque, d'y associer une localisation géographique et par extension une nationalité potentielle, rien ne garantit l'authentification des auteurs, voire des commanditaires ⁽⁷⁾. Les cyberattaques sont réalisées via des armes logiques ou cyberarmes, qui sont des applications

(2) Comme l'influence de la Russie sur l'élection du président Trump, cf. « The Perfect Weapon: How Russian Cyberpower Invaded the U.S », *The New York Times*, 13 décembre 2016 (www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html).

(3) Général BEAUFRE, *Introduction à la stratégie*, 1963.

(4) Le programme *Stuxnet*, dénommé aussi *Olympic Games*, qui a été réalisé par les États-Unis et Israël, en est un bon exemple car il a non seulement atteint sa cible – la centrale nucléaire iranienne de Natanz –, mais il s'est également propagé par *Internet*, affectant de nombreux systèmes informatiques dans d'autres pays (15 000 ordinateurs infectés)

(5) Le code de *Stuxnet* a été mis en ligne et chacun peut s'en servir en l'améliorant. Ceci aurait conduit à l'élaboration du virus *Duqu*.

(6) Le virus *Octobre rouge*, qui exploitait plusieurs failles au sein de Microsoft Word et Microsoft Office, fut lancé en 2007 mais découvert seulement en janvier 2013 par la société Kaspersky.

(7) La technologie *Virtual Private Network (VPN)* permet d'établir un « tunnel *VPN* » (un flux de données partant d'une adresse *IP* masquée) crypté vers un hôte (ou serveur) sur *Internet*. Ainsi, le flux est anonyme, sans restriction, impossible à intercepter car indétectable sur *Internet* indépendamment de la façon dont l'émetteur est connecté (réseau public ouvert, Wi-Fi, cyber cafés...). Au *VPN*, il faut également rajouter le navigateur The Onion Router (TOR).

logicielles multiformes. Elles s'étendent d'une application contrôlant une armée d'ordinateurs zombies pour attaquer un site ⁽⁸⁾ à une application (type virus ou ver) nécessitant la maîtrise ⁽⁹⁾ d'un haut niveau pluri-technique, conjuguée à une capacité de renseignement performante pour infecter la cible visée. Ainsi, par cette asymétrie du rapport défense/attaque, le cyberspace est plus propice à l'attaque qu'à la défense.

La caractérisation de l'agresseur lui-même révèle une typologie plus large que dans les conflits classiques. Les auteurs peuvent être des États, des organisations internationales ou nationales, des entreprises, des organisations criminelles ou terroristes, mais également des individus (militants, lanceurs d'alerte, *hackers*) qui peuvent déclencher une crise en quelques instants avec un *smartphone*. Sur ce dernier point réside la singularité du cyber sur les autres milieux, avec l'émergence de l'individu comme acteur direct. Ainsi, il existe une spécificité propre à la cyberconflitualité au travers de ses caractéristiques intrinsèques, l'extraterritorialité de son champ d'action et la multiplicité de ces acteurs.

Comment certains acteurs appréhendent leur souveraineté dans ce nouveau milieu : les facteurs clés ?

Les États-Unis où la prédominance d'un cyberpower...

L'histoire du cyberspace commence sur le seul territoire américain avec la création en 1969 d'Arpanet pour les besoins de la Défense, développé par la *Defense Advanced Research Projects Agency (DARPA)*, et la création du protocole *TCP/IP (Transmission Control Protocol/Internet Protocol)* en 1972. Pour son usage civil, *Arpanet* deviendra *Internet* avec la création des noms de domaine en 1983 et du *World Wide Web* en 1989. *Internet* sortira de l'espace américain avec le développement des réseaux dans le monde passant d'un million d'utilisateurs en 1992 au milliard quinze ans plus tard. Néanmoins, les normes techniques qui le structurent sont issues du corpus normatif américain : le code *ASCII (American Standard Code for Information Interchange)*, le protocole *TCP/IP* ou l'*OSI (Open System Interconnection)*. La couche physique du cyberspace est créée et dominée par les États-Unis au travers de l'*Internet Corporation for Assigned Names and Numbers (ICANN)* ⁽¹⁰⁾ et des 9 serveurs racines sur 13 localisés

(8) Selon le site *Journal du Geek*, depuis septembre 2016, des sociétés qui permettent le bon fonctionnement d'*Internet* (principalement des fournisseurs d'accès, mais aussi les sociétés qui s'occupent des infrastructures d'*Internet*) subissent de plus en plus fréquemment des attaques de type « *Distributed Denial of Service* » (*DDoS*) [déli de service distribué], afin d'identifier leur défense et surtout de vérifier leurs capacités de réaction. L'attaquant frappe, *via* un réseau d'ordinateurs (*botnet*) contrôlés à distance (à l'insu du propriétaire), les serveurs de requêtes que le défenseur se doit de filtrer pour assurer un service normal. Ces attaques permettent de savoir quelle bande passante maximum les défenseurs peuvent déployer pour contrer les attaques et la puissance nécessaire pour les faire tomber (ne plus assurer le service), et avec elle *Internet*. Voir Gaël WEISS, « La Chine ou la Russie tentent-elles de faire tomber *Internet* ? », *Journal du Geek*, 19 septembre 2016 (www.journaldugeek.com/2016/09/19/la-chine-ou-la-russie-tentent-elles-de-faire-tomber-internet/).

(9) *Hacking* par clé USB, la connaissance de vulnérabilités inconnues (« *zero-day* ») des systèmes d'exploitation, élaboration d'une ou plusieurs « charges utiles » permettant d'agir sur les systèmes de contrôle industriel et sur des automates programmables. Le ver *Stuxnet* qui a frappé les installations nucléaires iraniennes à l'été 2010 était conçu avec 4 « *zero-day* » et de 2 charges utiles, l'une déphasant les centrifugeuses, l'autre perturbant les systèmes de contrôle qui n'ont rien remarqué.

(10) De par le rôle de coordination qu'elle joue au sein du système d'attribution de noms *Internet*, elle exerce une influence non négligeable sur le développement et l'évolution du *Web*. L'*ICANN* est à l'origine une organisation de droit californien. Cela signifie qu'elle devait se conformer à la législation des États-Unis et qu'elle pouvait être amenée à rendre des comptes au système judiciaire – en d'autres termes, l'*ICANN* peut être poursuivie en justice. C'est également une société

sur le territoire américain. Les normes restent par essence un enjeu géopolitique, comme en témoigne l'ouverture sous la pression internationale en octobre 2009 des noms de domaine au cyrillique, à l'arabe et au mandarin, mettant fin à l'hégémonie de la graphie américaine (alphabet latin sans accentuation). Les acteurs privés américains du secteur informatique restent également de premier plan pour les composants (Intel, NEC) et les équipements pour particuliers ou entreprises (IBM, Compact, Ericsson). La concentration de ces acteurs sur un marché domestique sans concurrence leur permet de s'allier et de définir eux-mêmes les nouvelles normes internationales. De plus, *via* les GAFA (Google, Amazon, Facebook, Apple), les États-Unis ont également une position dominante dans la couche logicielle au vu du taux de pénétration de leurs applications ⁽¹¹⁾. Ils disposent d'un système d'exploitation national, voire mondial ⁽¹²⁾ au travers de Windows, auquel la NSA (*National Security Agency*) aurait participé pour la version Windows Vista et Windows 7. Depuis 2011, la NSA contribue également au code d'Android sous la forme d'instructions appelées *Security Enhancements for Android*, renforçant le doute sur l'existence de portes dérobées informatiques permettant d'analyser ou de prendre le contrôle à distance de serveurs ou terminaux mobiles. La couche informationnelle occidentale est également dominée par les États-Unis par l'exploitation économique des données de masse et de la valeur ajoutée qui s'en dégage.

Le premier texte doctrinal de la vision américaine du cyber, l'*International Strategy for Cyberspace*, considéré comme 5^e milieu, est publié par l'exécutif en mai 2011. Basé sur trois piliers (défense, développement économique et diplomatie), il précise que la prédominance technique doit non seulement protéger les États-Unis des diverses menaces mais également permettre la diffusion des valeurs libérales américaines (libertés fondamentales, respect de la propriété et de la vie privée ⁽¹³⁾, libre circulation de l'information ⁽¹⁴⁾...), grâce à un *Internet* universel, libre, stable, ouvert et interopérable, basé sur un usage collectif où chacun doit avoir un comportement « acceptable » et « responsable ». L'accent est mis sur l'innovation technologique pour conserver l'avance sur les adversaires. Ce texte évoque la dissuasion, capacité à résister aux attaques sur le sol américain ou à l'étranger, grâce à des coopérations étroites au sein d'un concept de dissuasion collective. Il évoque également le terme de *deterrence*, capacité de riposte américaine. Les États-Unis continueront à renforcer leurs alliances et à accroître les coopérations militaires au sein desquelles ils conserveront un rôle

d'utilité publique à but non lucratif, et ses « directeurs » ont l'obligation légale de s'acquitter de leurs devoirs aux termes du droit des sociétés. Jusqu'au 30 septembre 2016, on pouvait considérer cette organisation sous l'influence du département du Commerce américain puisque c'est une organisation de droit californien devant respecter le droit américain des sociétés. Voir « Quel est le rôle de l'ICANN ? », *ICANN.org* (www.icann.org/resources/pages/what-2012-02-25-fr).

(11) Les navigateurs : Internet Explorer, Chrome ; les moteurs de recherche : Google, Bing, Duckduckgo.

(12) Cf. Emilien ERCOLANI, « La part de marché Windows sous les 90 % ! », *L'informaticien*, 2 décembre 2008 (www.linformaticien.com/actualites/id/5410/la-part-de-marche-windows-sous-les-90.aspx).

(13) Le *Patriot Act* mis en place sous l'Administration Bush confère aux autorités policières et judiciaires de très nombreux et puissants pouvoirs en matière de cybercriminalité qui outrepassent le respect de la vie privée. De même, la France avec la loi Hadopi possède des outils de contrôle parmi les plus sophistiqués au monde qui peuvent s'apparenter à une censure d'*Internet*.

(14) L'affaire Snowden, en juin 2013, met en lumière l'ampleur de la surveillance mondiale exercée par les États-Unis sur les communications internationales à des fins géopolitiques, lançant d'autres Nations (Chine, Russie) dans la course à l'acquisition de ces mêmes capacités

prépondérant. Cette stratégie est complétée par deux documents du département de la Défense (*DoD*) : le *Strategy for Operating in Cyberspace* ⁽¹⁵⁾ de juillet 2011 et le *Cyberspace Policy Report* de novembre 2011. Ils indiquent que toute cyberattaque fera l'objet d'une réponse offensive incluant si nécessaire des moyens conventionnels et que les États-Unis élargiront leurs coopérations formelles et informelles à un ensemble d'alliés et de partenaires. Ces documents parlent de « défense active ». L'exécutif américain se verrait également, selon un article du *New York Times* de février 2013¹⁶, doté de vastes pouvoirs en matière de riposte et de déclenchement d'opérations préventives dans le cyberspace sans devoir être en état de guerre, relançant le concept de guerre préventive. Il s'appuiera sur l'*US Cybercom*, créé fin 2010, en charge de réagir aux attaques informatiques, lutter contre le terrorisme informatique et mener des offensives dans le cyberspace. Enfin, le 20 février 2013, l'Administration Obama publiait également la *Stratégie de l'administration sur l'atténuation des vols de secrets commerciaux américains*, formalisant en termes de représailles économiques la réaction américaine à des agressions étatiques.

Ces publications permettent de formaliser le concept de *cyberpower* de Joseph Nye qui complète le *soft and smart power*. La dimension informationnelle du cyberspace est abordée sous l'angle de la prédominance de la diplomatie américaine, conjuguée aux actions d'acteurs économiques américains dominants qui ont bien perçu, dès la fin des années 1990, l'émergence d'une nouvelle économie qui exploitera les données de masse et les informations qu'elles contiennent pour créer la valeur ajoutée de demain. Cette avance conceptuelle sur l'Europe a été cruciale.

... face à la volonté russo-chinoise d'un retour de leur souveraineté...

À l'opposé de l'approche technologique ou techniciste américaine, l'approche russe s'enracine dans le choc civilisationnel issu de la disparition de la Russie de Kiev et des trois siècles sous le joug mongol. Cette occupation vit l'émergence de la Moscovie et de son extension territoriale jusqu'aux limites de la Russie contemporaine, ainsi que d'une conscience géopolitique bicéphale orient/occident. En réponse à son passé, la pensée russe recherche en permanence à garantir la sauvegarde de l'entité politique, sociale, culturelle et culturelle du pays, le respect de son intégrité territoriale et de sa souveraineté. Dans le cyberspace, vu comme un espace informationnel, l'essentiel pour la Russie est donc de se garantir une sécurité informationnelle à la fois par le contenant et par le contenu. Le gouvernement chinois, quant à lui, a créé avec la même ambition un espace séparé proprement chinois sous forme d'un *Intranet* national avec une barrière technique, sorte de « Grande muraille électronique » ou « Grand *Firewall* de Chine », pour bloquer le routage d'adresse *IP* ou filtrer des noms de domaine (*DNS*).

En termes de doctrine, le texte fondateur de la cyberstratégie russe ⁽¹⁷⁾, la *Doctrine de sécurité informationnelle de la Fédération de Russie*, est publié le

(15) Stéphane DOSSÉ, Olivier KEMPF et Christian MALIS, *Le Cyberspace – Nouveau domaine de la pensée stratégique*.

(16) Philippe BERNARD, « États-Unis : vers une réglementation secrète contre les cyberattaques », *Le Monde*, 4 février 2013 (www.lemonde.fr/).

(17) Yannick HARREL, *La cyberstratégie russe*.

9 septembre 2000 et pose les bases de la stratégie informationnelle russe. Il émane du Conseil de sécurité de la Fédération de Russie. C'est un texte-cadre pour l'ensemble des services de l'État et non pour la seule communauté du renseignement. Le regroupement des termes stratégie, espace et sécurité informationnels est centré sur le rôle majeur de l'information. Le terme « informationnel » regroupe dans la pensée russe les trois couches du cyberspace évoquées *supra* incluant par ailleurs un volet « civilisationnel » lié à leur histoire. Pour les autorités, la vraie menace est la vulnérabilité de la population aux influences extérieures en imaginant des menaces qui se sont concrétisées dix ans plus tard.

Il est fait mention également d'éléments ayant trait tant au domaine matériel que logiciel et il s'inscrit dans la nécessité de développer une industrie propre, sous le statut, pour certaines, d'entreprises stratégiques ⁽¹⁸⁾ afin d'asseoir la souveraineté du pays. Ce document cadre prévoit également « l'emploi d'une certification de la sécurisation des données et de leur authentification » par les entreprises nationales lorsqu'elles utilisent massivement des logiciels étrangers. Il insiste sur la reconnaissance juridique de la sécurité de l'espace informationnel afin de garantir son intégrité et sa transmission vers l'individu, le corps social et l'État, ainsi que les normes spécifiques associées. La construction d'infrastructures informationnelles et la promotion d'une indépendance de la défense par le déploiement d'un système de Technologie de l'information et de la communication (TIC) spécifique, sont également citées.

Ces objectifs sont confortés en novembre 2013 par la parution de la *Stratégie de développement de l'industrie des technologies de l'information dans la Fédération de Russie pour 2014-2020 et perspectives à l'horizon 2025*, qui analyse les résultats obtenus depuis 2000 pour accentuer la nécessité de faire émerger des entreprises nationales en matière de TIC. Il préconise de s'appuyer sur le complexe militaro-industriel pour pérenniser le niveau national puis conquérir des marchés à l'international. La doctrine de 2000 est complétée par une doctrine militaire publiée en 2010, puis complétée en 2012, *Les visées conceptuelles des forces armées dans l'espace informationnel*. Dans ce document, la sécurité informationnelle regroupe la cyberdéfense et la cybersécurité. Il mentionne la guerre informationnelle et les besoins offensifs et défensifs de l'armée russe pour y faire face. L'équivalent d'un cyber-commandement américain a été mis en place en février 2013 au sein de l'État-major russe, en charge de la sécurité de l'information des forces armées et de l'infrastructure de l'État.

A contrario de l'approche russe, il est difficile de caractériser la doctrine chinoise car il n'y a pas de publication. Le seul texte de référence est *La guerre hors limite* des officiers Quia Liang et Wang Xiangsui où le contrôle de l'information est un moyen stratégique pour remporter la victoire sans verser de sang. La cyberstratégie chinoise est donc axée sur la suprématie informationnelle sous toutes ses formes. Dans le *Livre blanc sur la stratégie militaire* de mai 2015, le cyberspace est à la fois un nouveau pilier du développement économique et social, mais également un nouveau domaine

(18) Entreprises russes sous la protection du gouvernement comme Sistema (télécommunication) et sa filiale Sitronics (infrastructures et composants micro-électroniques), Vimpelcom et sa marque Beeline (opérateur mobile)

de la sécurité nationale. Il met l'accent sur la défense active, sur l'augmentation des capacités dans la perception de la situation du cyberspace, la cyberdéfense, et sur la cybercoopération internationale en vue de prévenir les crises du cyberspace, de garantir la sécurité du cyberspace et de l'information, de sauvegarder la sécurité nationale et la stabilité sociale. Néanmoins, les réflexions stratégiques chinoises ont comme impératif la survie du régime par le contrôle de l'information dans tous les domaines.

Le développement de la force de frappe balistique intercontinentale soviétique et de la conquête spatiale a permis l'émergence des prémices de la couche physique du cyberspace russe, par le développement d'une industrie électronique et d'une série de supercalculateurs ⁽¹⁹⁾. Sur l'espace géographique de la Communauté des États indépendants (CEI), hors Ukraine, un *Runet*, ou « segment russe de l'*Internet* », apparut à la fin des années 1980 sous la forme première du réseau non automatisé *Demos*. Ce *Runet* se caractérise aujourd'hui par ses propres infrastructures, ses câbles, ses moyens de transport de l'information et ses points de passage avec le reste de la couche physique d'*Internet*. Il est actuellement « fibré » à plus de 40 % et est l'un des plus rapides du monde. Son contenu est principalement russophone avec des réseaux sociaux nationaux tels que *Vkontakte* et *Odnoklassniki*, dont les serveurs sont en Russie. Une collaboration russo-chinoise s'est également mise en place ces dernières années pour le développement des nouvelles générations de supercalculateur. En 2016, la Chine détenait le plus puissant d'entre eux. Elle est également en position dominante sur les routeurs ⁽²⁰⁾ de cœur de réseaux jusqu'aux terminaux mobiles.

Après l'effondrement des années 1990, l'excellence de la formation des ingénieurs russes a servi de matrice à l'émergence dans la couche logicielle de sociétés russes de sécurité informatique mondialement connues : *ERPScan* et *Kaspersky*, qui deviennent des acteurs indirects du jeu géopolitique entre États par l'identification des créateurs de virus. Un dispositif juridique est également apparu pour encadrer et protéger ces nouvelles sociétés de toute immixtion étrangère ⁽²¹⁾, voire de les utiliser ⁽²²⁾, le cas échéant, dans le domaine du cyberespionnage. Ainsi une proximité de ces sociétés avec les services de renseignement est indéniable. La Russie a développé ses propres moteurs de recherche, *Yandex* (60,5 % des recherches sur *Internet*) et *Rambler*, concurrents de *Google* qui ne règne pas en maître sur le marché russe à la différence du marché européen. Depuis 2011, un système d'exploitation national est en cours de développement ⁽²³⁾ sur la base du système ouvert *Linux* accessible plus facilement par ses services de renseignement au nom de la sécurité nationale. La Russie a annoncé également en

(19) BESM (1953) jusqu'au modèle 6 (1965, 1 million d'instructions/seconde), Elbrous, SKIF, MGU (2008, 60 téra-flops), SKIF Grid, SKIF Soyouz (2014, pétaflops).

(20) Les routeurs des sociétés Huawei et ZTE sont suspectées en octobre 2012 par la Commission du renseignement du Congrès américain d'atteinte à la sécurité informationnelle du pays en termes de capacités de fuite informationnelle au travers de dispositif de surveillance implanté par le fabricant.

(21) La « Loi pour la confiance dans l'économie numérique » indique que l'usage et la commercialisation d'outils de cryptage sont libres à la condition d'avoir été agréé préalablement par les services du Premier ministre. *Skype* et *Gmail* sont rentrés dans le champ de cette loi en 2011 puisque le *FSB* (Service fédéral de sécurité de la Fédération de Russie) ne pouvait vérifier la teneur des conversations cryptées.

(22) La loi fédérale russe oblige toute personne morale russe à apporter son concours aux services de renseignement à leur demande.

(23) « La Russie veut créer son propre système d'exploitation », *Le Monde*, 27 octobre 2010 (www.lemonde.fr/).

2015 qu'elle s'engageait dans un programme de développement d'un OS mobile, en partenariat avec la *start-up* finlandaise Jolla, sur une version nationale de SailFish OS avec pour objectif de ramener la part des OS Android et iOS sur le marché russe de 95 à 50 % d'ici 2025.

Comme la Russie, la Chine a développé dans sa couche logicielle une offre alternative aux sites *Web* les plus répandus au sein d'un marché intérieur protégé de toutes concurrences étrangères. Des équivalents chinois des sites étrangers ont vu le jour comme Baidu (Google), Alibaba (Amazon), WeChat (Facebook + WhatsApp + SMS), Weibo (Twitter), QiYi (YouTube). À terme, le BAT (Baidu, Alibaba, Tencent) chinois pourra défier à l'extérieur l'hégémonie américaine des GAFAs, en s'appuyant sur un marché intérieur captif et protégé. Un programme de développement d'un système d'exploitation souverain baptisé COS (China Operating System) a été lancé par la Chine en 2014, afin de s'affranchir de la suprématie américaine. Les entreprises chinoises, à l'image de la société Tencent (WeChat), coopèrent très étroitement avec le gouvernement pour contrôler toute cyberdissidence et maîtriser la couche informationnelle.

Cependant, la Chine essaie de combler son retard par un espionnage industriel et militaire massif. À cet effet, elle a concentré au sein de l'Armée populaire de libération (APL) la totalité de ses capacités étatiques ⁽²⁴⁾, tant défensives (contre-influence) qu'offensives (influence, espionnage et intrusion), et a développé une collaboration étroite avec des *hackers* pour s'emparer des technologies étrangères. Le service de renseignement militaire (*GRU*) russe dispose de moyens ⁽²⁵⁾ analogues en matière de cyber-espionnage et d'influence qui ont défrayé la chronique ⁽²⁶⁾ lors de l'élection de Donald Trump à la présidence américaine. Il s'appuie également sur des structures cybercriminelles professionnelles, en échange d'un certain laxisme juridique sur leurs autres activités. Par analogie avec le milieu maritime, les États russe et chinois utilisent une flotte de corsaires et de pirates *hackers* tout en contrôlant les voies de communication de leur espace informationnel (*Runet*) ou en défendant leur bande côtière (Grande muraille électronique).

...et une approche française au sein de l'UE

L'approche française du cyberspace est centrée sur la cyberdéfense et la cybersécurité. Le *Livre blanc sur la Défense et la Sécurité nationale* de 2008 identifie, parmi les nouvelles menaces, l'attaque majeure étatique ou non étatique contre les systèmes d'information. Cette stratégie s'accompagne d'une volonté de développer au sein de l'UE une coopération opérationnelle la plus réactive possible entre États partenaires face aux attaques, et de favoriser la montée en gamme des autres pays de l'UE en cyberdéfense. En matière de sécurité des systèmes d'information, la France doit garder un domaine de souveraineté concentré sur les capacités nécessaires au maintien de

(24) Dont l'unité 61 398 en charge d'attaques sophistiquées persistantes (*APT*) identifiée par le rapport de la société de sécurité informatique Mandiant en février 2013.

(25) Dont l'unité baptisée « Fancy Bear » par la société de cybersécurité CrowdStrike en décembre 2016.

(26) Ellen NAKASHIMA, « Cybersecurity firm finds evidence that Russian military unit was behind DNC hack », *The Washington Post*, 21 décembre 2016 (www.washingtonpost.com/).

l'autonomie stratégique et politique de la Nation. À cet effet, le gouvernement a créé l'Autorité nationale de défense des systèmes d'information (ANSSI) en 2009, et a publié en 2011 la stratégie de la France en matière de défense et de sécurité des systèmes d'information. Ce texte déclinaît quatre objectifs stratégiques dont la protection de l'information de souveraineté⁽²⁷⁾ et le renforcement de la cybersécurité des infrastructures vitales nationales⁽²⁸⁾.

Le *Livre blanc* de 2013 a confirmé l'analyse précédente des menaces cyber. La « capacité de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs est devenue un des éléments de la souveraineté nationale ». D'autre part, « la capacité de produire en toute autonomie des dispositifs de sécurité, notamment en matière de cryptologie et de détection d'attaque, est à cet égard une composante essentielle de la souveraineté nationale ». La position française repose sur la mise en place d'une posture robuste et résiliente de protection des Systèmes d'information (SI) de l'État, des Opérateurs d'importance vitale (OIV) et des industries stratégiques. En cas d'attaque caractérisée, la doctrine prévoit une « capacité de réponse gouvernementale globale » faisant appel à l'ensemble des moyens régaliens de l'État, sans « s'interdire l'emploi gradué de moyens relevant du ministère de la Défense, si les intérêts stratégiques nationaux étaient menacés ».

Une première approche de la couche informationnelle émerge en 2015 avec la *Stratégie nationale pour la sécurité numérique*, fruit de travaux interministériels coordonnés par l'ANSSI. Elle aborde la « captation de richesses numériques », composées en partie de nos données personnelles et de notre vie privée, et « des formes sophistiquées de propagande ou d'orientation des convictions ou des habitudes ». La maîtrise de ces masses de données est un enjeu de défense et de sécurité nationale, donc de souveraineté.

Une feuille de route vers un modèle de souveraineté 2.0

Une nécessaire première pierre...

Pour pouvoir exercer une souveraineté dans le cyberspace, il faut que cette dernière soit reconnue dans le droit international. En 2013, le Groupe d'expert gouvernementaux (GGE) de l'ONU s'est prononcé positivement sur l'application du droit international et de la charte de l'ONU au cyberspace, et par voie de conséquence sur la reconnaissance d'une souveraineté. Cette proposition a été acceptée par un certain nombre de pays dont la Chine. Néanmoins aucune définition du périmètre de cette souveraineté n'a été apportée.

Pour la caractériser dans le cyberspace et face aux enjeux géopolitiques des normes et des comportements, il est nécessaire de s'interroger sur la gouvernance « de »

(27) Fraction de l'information diplomatique, militaire, scientifique, technique et économique qui permet notre liberté d'action.

(28) Protection des réseaux de communications électroniques utilisant *Internet*, comme la sécurisation des systèmes critiques des opérateurs d'importance vitale, face aux intrusions visant à recueillir des informations scientifiques et technologiques ou à tester la vulnérabilité des protections en place.

(au niveau technique) et « sur » (au niveau des internautes) *Internet*, ainsi que sur la place exclusive des États. Pour la gouvernance d'*Internet*, et même si l'*ICANN* n'est plus sous la coupe du département du Commerce américain (*DoC*) depuis le 30 septembre 2016, cette organisation doit néanmoins évoluer vers une organisation à personnalité internationale dotée d'une gouvernance intergouvernementale, qui reprendrait le contrôle de l'organisation et du nommage d'*Internet* vis-à-vis d'acteurs privés dominants.

Pour la gouvernance sur *Internet*, une charte ⁽²⁹⁾ ou code de bonne conduite a été proposé lors de la 66^e session de l'Assemblée générale des Nations unies par la Russie et la Chine le 14 septembre 2011. Une proposition similaire a été renouvelée un an plus tard lors de la conférence de l'Union internationale des télécoms (UIT) à Dubaï en décembre 2012. Ces propositions ont été rejetées par les États-Unis. Deux visions d'*Internet* s'opposent, traduisant un affrontement géopolitique centré sur un changement de gouvernance du cyberspace : l'une, menée par les États-Unis, qui considèrent qu'*Internet* est un espace de libre circulation, mais sous leur prédominance bienveillante, et l'autre, menée par la Russie et la Chine, qui veulent plus de contrôle étatique, face aux influences extérieures et intérieures sur leurs populations. Un nouveau code de bonne conduite a été proposé en 2015 par l'Organisation de coopération de Shanghai (OCS), mais la notion de « sécurité informationnelle » évoquée traduisait toujours la volonté irrecevable d'un contrôle de la population.

Néanmoins, la place des États dans une régulation intergouvernementale doit être impérativement recherchée. Le contexte international y est favorable grâce à une convergence d'intérêts entre un bloc russo-chinois qui le demande, des pays émergents qui ne veulent plus se faire imposer des normes américaines et une Union européenne qui commence à prendre conscience de l'existence de son espace informationnel. Cette régulation est la première pierre nécessaire à la reconnaissance d'une souveraineté numérique.

...complétée par un « Montego Bay » du cyberspace...

Le deuxième élément caractérisant une souveraineté est la reconnaissance de la place de la donnée dans le droit international. En effet, la donnée est au cœur de la souveraineté en tant que ressource stratégique du pays d'où elle émane. Il est donc nécessaire d'inscrire dans le droit la notion de « propriété des données informatiques personnelles », en tant que « bien attribué à celui qui en est à l'origine ». Selon sa valeur

(29) Ce texte abordait 6 points majeurs : 1° la nécessité de collaborer avec les instances internationales, en premier lieu avec l'ONU ; 2° l'obligation de préserver le cyberspace de toute prolifération d'armes informationnelles et de technologies connexes ; 3° la coopération en matière de lutte contre les activités criminelles et terroristes œuvrant sur les réseaux sociaux et propageant des idées incitant au terrorisme, au sécessionnisme, à l'extrémisme, ou tentant de déstabiliser un pays sur les plans politique, économique et social, mais aussi culturel et cultuel ; 4° le droit pour chaque pays de prendre toute mesure, conformément aux lois et aux réglementations, pour protéger son espace et ses infrastructures informationnelles les plus sensibles des perturbations, attaques et actes de sabotage ; 5° la liberté de chercher, de consulter et de diffuser des données informationnelles garantie au regard du respect de la législation nationale ; 6° (le plus crucial) la gouvernance d'*Internet* et le partage des responsabilités, notamment la gestion partagée des noms de domaine réalisée par l'*ICANN*, organisation sous l'influence du *DoC*.

informationnelle, cette donnée permet une prise de décision stratégique qui influencera notre société dans différents domaines.

Bien que des normes de comportement stabilisateur aient été proposées en 2015 par le GGE de l'ONU, la formalisation de différentes obligations mutuelles entre États est impérative. La transposition au cyberspace du principe de « *due diligence* », qui détermine qu'« aucun État n'a le droit d'utiliser ou de permettre l'utilisation de son territoire de manière à causer un préjudice sur le territoire d'un autre État », est un premier axe. Ce principe est aussi mis en avant dans le *Manuel de Tallinn*, qui propose l'existence d'un « devoir à la charge des États de prévenir les actes illégaux commis dans le cyberspace à partir de leur territoire ». Il est également légitime de pouvoir bénéficier d'un droit de poursuite pour lutter contre les corsaires ou pirates (*hackers*) des temps modernes. En s'appuyant sur certaines propositions du code de « bonne conduite » russo-chinois cité *supra*, comme sur la Convention sur la cybercriminalité (dite de Budapest) du Conseil de l'Europe de novembre 2001, la lutte contre la prolifération et la cybercriminalité sur *Internet* représente un autre volet devant être admis par tous.

Pour permettre de transcrire ces différents principes ou obligations, la France doit promouvoir l'élaboration d'une convention internationale ou « Montego Bay » du cyberspace, auquel la Russie et la Chine ne pourraient s'y opposer par convergence d'intérêts. Seuls les États-Unis pourraient y voir une menace pour la prédominance de leur modèle économique numérique, mais leur position serait difficilement tenable face à une alliance objective de différents blocs.

...et une souveraineté partagée au sein de l'Europe...

En s'appuyant sur la puissance normative de l'UE, la France doit promouvoir les notions de souveraineté numérique étatique et européenne ainsi qu'un cadre réglementaire et financier associé. Grâce à des éléments clés des champs matériel, logiciel et informationnel constitutifs d'une souveraineté numérique et que nous développerons ultérieurement, il serait nécessaire de séparer ceux relevant exclusivement de l'État, par extension par exemple du périmètre de l'article 346 du Traité sur le fonctionnement de l'UE, de ceux qui seraient abandonnés par l'État au profit de l'UE.

Comme au niveau international, l'élément clé de la souveraineté européenne est la place de la donnée. Elle devra être considérée comme une pièce maîtresse de cette souveraineté en établissant un droit européen de l'information personnelle. L'individu redevient le centre de gravité de l'économie numérique européenne en se réappropriant ses données, qui regroupent l'intégralité de sa trace informatique. À cet effet, l'UE devra renoncer à l'accord euro-américain « Privacy Shield »⁽³⁰⁾ de transfert de données de l'UE vers les États-Unis et imposer que toute donnée concernant un ressortissant de l'UE devra être stockée, traitée et analysée sur le territoire d'un État-membre de l'UE.

(30) Accord du 12 juillet 2016 conclu entre la Commission européenne et les États-Unis, devant se substituer au Safe Harbor, autorisant les transferts de données depuis l'UE vers les États-Unis opérés avec des entreprises américaines certifiées auprès des autorités américaines.

... qui s'appuie sur des facteurs de puissance...

L'élaboration d'une stratégie nationale spécifique au numérique formaliserait le développement de facteurs de souveraineté étatique, qui seront aussi des facteurs de puissance au sein des trois couches du cyberspace.

En s'appuyant sur Bpifrance et un important écosystème de sociétés françaises du numérique déjà existant, le premier facteur de puissance est la constitution d'une Base industrielle et technologique du numérique (BITN) capable de produire des matériels et des logiciels sur des segments définis comme enjeux de notre souveraineté : technologie quantique et calcul intensif, intelligence artificielle, objet connecté, analyse des données de masse, *blockchain*, sécurisation du fonctionnement numérique d'OIV... Cette base regrouperait des entreprises de différentes tailles allant de la *start-up* innovante, devant être accompagnée pour son développement et protégée de la prédation d'entreprises étrangères dominantes, jusqu'à l'entreprise de taille européenne ou internationale. Elle pourra également développer des offres sur les marchés concurrentiels internationaux, sachant que la partie relevant de la souveraineté serait « encapsulée » au sein de l'entreprise, afin de protéger le potentiel scientifique et technique stratégique français. La bataille de la première étape de la révolution numérique lancée au début des années 1990, représentée par la technologie et les applications actuellement utilisées au sein des couches physique et logicielle, a déjà été perdue. La reconquête de notre autonomie dans les prochaines technologies de seconde génération nécessite d'être préparée. À cette fin, le développement de différents segments stratégiques synonymes d'une autonomie reconquise devra être recherché.

Sur les segments stratégiques des routeurs de cœur de réseau et d'un système d'exploitation (ou OS) « maîtrisé » de nouvelle génération lié aux avancées de la couche physique et sous différentes versions (mobiles, terminaux et objets connectés), l'État devra s'y investir directement. Ce système d'exploitation devra être utilisé par les OIV dans un premier temps. Il permettra par exemple d'éviter une fuite d'éléments sensibles vers les serveurs américains (cartographie de configuration réseau demandé par Microsoft pour bénéficier des mises à jour de sécurité), mais il doit également constituer une offre concurrentielle.

Les caractéristiques attendues pour la mise en place d'un *cloud* souverain sont également un facteur de souveraineté lié à l'accès, au stockage et à la protection des données. Ce *cloud* permettra le stockage de données de plus en plus externalisées (données de ressources humaines,...) et celles considérées comme stratégiques au titre du potentiel scientifique et technique. La piste d'un *cloud* à deux niveaux pourrait être utilement analysée. Un *cloud* à vocation nationale pour les entreprises stratégiques en s'appuyant sur les compétences de la société française OVH (1^{er} hébergeur européen et 2^e mondial), et un maillage de *cloud* à vocation régionale au niveau des collectivités territoriales, comme offre de proximité pour les PME et PMI. La mise en place d'un *Intranet* national résilient devrait également être étudiée à partir des capacités et infrastructures existantes de la société Orange, l'accélération du déploiement de la fibre optique sur l'ensemble du territoire, l'analyse du réseau hertzien actuel et la potentialité

de la technologie radio « *ultra narrow band* » diffusée par le réseau de la société française Sigfox pour l'*Internet* des objets (IdO).

Sur le segment stratégique des moteurs de recherche, le moteur français Qwant, conçu en février 2013 par une *start-up* niçoise, devrait être soutenu, imposé dans l'administration et les OIV et diffusé le plus largement possible au niveau européen. Ainsi des alternatives au GAFa ou BAT existent. Il est nécessaire de les identifier et les soutenir pour les faire croître.

...dans un environnement structuré...

Le développement d'un dispositif d'intelligence économique axé sur l'économie numérique est un impératif qui serait également l'un des objectifs de la stratégie nationale, afin d'orienter à la fois la recherche mais également de détecter au plus tôt nos « pépites » innovantes pour les inclure dans cette base industrielle.

Il est impératif de développer nos réflexions et d'adapter notre stratégie nationale pour se préparer aux prochaines étapes de la révolution numérique. Une pensée stratégique existe, mais elle n'est pas aujourd'hui fédérée pour faire face aux enjeux à venir. Pour atteindre cet objectif, un Conseil national de recherche sur le numérique centré sur le monde académique devrait être créé. Son action compléterait les champs de réflexion du Conseil national du numérique centré sur les élus, la société civile et le monde économique. Il appuierait également notre diplomatie du cyberspace en formant avec le Conseil national du numérique des « délégations technologiques », à l'instar des délégations technologiques américaines, associant la Silicon Valley et le Département d'État.

Les partenariats sont également un autre enjeu majeur du développement du numérique et d'une réponse toujours la plus adaptée à ses évolutions rapides. Il serait nécessaire de développer des partenariats avec les industriels dans les champs matériels et logiciels, mais également avec le monde universitaire pour comprendre et se préparer aux futures évolutions, pour faire émerger un vivier d'expert et des filières de formation dans le cyber. Le développement de partenariats bilatéraux ou multilatéraux sur des projets numériques et sur l'élaboration de normes européennes devrait être entrepris. Pour les promouvoir, il serait souhaitable de s'appuyer sur le volet « capacités » du Fonds européen pour la défense, créé par le Plan d'action européen de la défense (EDAP) de la Commission européenne.

...où une souveraineté informationnelle doit être reconquise...

Les entreprises américaines qui ont accompagné l'émergence d'*Internet* ont eu le temps de penser et façonner le cyberspace comme un nouveau champ économique. En s'appuyant sur le marché américain, les logiciels des GAFa ont conquis assez rapidement une position dominante dans le monde occidental, afin d'être en mesure de capter la valeur ajoutée économique du traitement de la donnée. Ainsi, un des premiers objectifs du Conseil national de recherche sur le numérique consisterait à formaliser les

enjeux de la sphère informationnelle dans le développement de l'économie numérique et d'étudier son impact sur l'économie « traditionnelle ».

Dans la couche informationnelle, il ne faut pas exclure la dimension humaine et le champ des perceptions. C'est un nouveau champ de conflictualité où la propagande s'y est développée. Au travers de forums puis des réseaux sociaux, des organisations islamistes ont investi ce nouvel espace de communication pour propager le djihadisme *via* des plateformes opérationnelles de téléchargement de manuels du parfait djihadiste, promouvoir un modèle sociétal religieux et recruter des combattants. Au-delà des manœuvres offensives de nos services sur la toile, du blocage, de la suppression et de la censure que nos textes de loi permettent, le champ des perceptions ne doit plus être abandonné, mais un discours alternatif doit être construit autour d'un message, d'un messenger et d'un vecteur. Des réponses publiques existent (site gouvernemental « stop djihadisme », numéro vert de signalement d'une radicalisation), mais elles doivent également être sociétales. Il est nécessaire de faire émerger un contre discours associatif ou d'initiative citoyenne. Il pourra s'appuyer sur des campagnes de type « *Online Civil Courage Initiative* » conçues par l'*Institute for Strategic Dialogue* de Londres et aidés par Facebook pour cibler une population réceptive à la propagande djihadiste. Des vidéos de témoignage de parents, de proche, de victimes françaises ou étrangères, de repentis peuvent également être réalisées et utilisées sur YouTube *via* « *the Redirect Method* » de Google, pour présenter systématiquement un référentiel alternatif aux vidéos de propagande djihadiste. Les collectivités territoriales peuvent être des « facilitateurs » pour permettre la rencontre entre les associations et Facebook ou Google, mais sans jamais apparaître pour ne pas brouiller le message ou l'image de l'initiative citoyenne. Il faut enfin obtenir des grandes sociétés du *Web* qu'elles assument leur responsabilité dans cette lutte en chassant et supprimant les comptes et les contenus promouvant le djihadisme.

Un Commissariat à l'espace numérique et aux nouvelles technologies

Au-delà des enjeux de cyberdéfense et de cybersécurité formalisés dans les deux derniers *Livres blancs, dans la stratégie nationale pour la sécurité du numérique* de 2015 et par une doctrine présentée par le ministre de la Défense, Jean-Yves Le Drian, le 12 décembre 2016 à Bruz, la France doit développer une « politique globale de souveraineté numérique ». Elle définirait nos ambitions internationales, une stratégie nationale⁽³¹⁾ et un plan d'actions avec des propositions adaptées aux enjeux des trois couches sur la base des différents éléments développés *supra*. Pour la mettre en œuvre et la personifier, il est nécessaire d'identifier un nouvel acteur qui serait le bras armé de cette ambition nationale. Il pourrait prendre la forme d'un Commissariat à l'espace numérique et aux nouvelles technologies, conseiller du gouvernement pour le numérique.

Afin d'assurer une cohérence organisationnelle, ce commissariat aurait également la responsabilité de la cybersécurité de nos OIV. À cet effet, l'ANSSI lui serait rattachée, tout en préservant un lien avec le cybercommandement (Cybercom) de

(31) En refondant la stratégie numérique du Gouvernement V1.0 ou république numérique en actes (juin 2015).

l'État-major des armées (EMA). Pour la lutte informatique, il aurait la responsabilité de développer en régie ou par certaines entreprises de la BITN des moyens d'analyse de composants et de virus, des plateformes collaboratives nécessaires à notre cyberdéfense, dont le client sera le Cybercom. À ce titre, les éléments de la DGA/Maîtrise de l'information travaillant dans ce domaine à Bruz (Ille-et-Vilaine) devraient lui être rattachés. Pour éviter les doublons, ce Commissariat travaillerait également en étroite collaboration avec la division des applications militaires du CEA, en charge de la simulation et du calcul intensif pour notre dissuasion nucléaire et de la DGSE pour la cryptographie et la cryptanalyse.

Pour pouvoir être efficace, il devrait être responsable d'un programme budgétaire propre au sens de la LOLF (loi organique relative aux lois de finances) et s'appuyer sur une évolution juridique du périmètre des entreprises considérées comme « stratégiques »⁽³²⁾. Ce statut lui permettrait d'empêcher tout rachat d'entreprise dite stratégique sans son aval. Un régime dérogatoire au code des marchés publics en lien avec ce statut devrait également être mis en place. Ce commissariat aurait en charge le développement des facteurs de souveraineté cités *supra*, l'accroissement de pôles de recherche dans les segments stratégiques, la mise en place d'un environnement structuré : Conseil national de recherche sur le numérique et partenariats. Il pourrait s'appuyer sur des financements à conquérir auprès du volet « recherche » du Fonds européen pour la défense, ainsi que l'inscription de certains segments au programme de recherche consacré à la défense, qui sera mise en place au titre du cadre financier pluriannuel de l'UE *post-2020*.

*

**

En conclusion, la reconquête d'une souveraineté numérique n'est pas une utopie, mais le fruit d'une ambition politique, s'appuyant sur une stratégie d'ensemble et des actions au niveau de l'Europe, de l'État, des collectivités territoriales, de la société civile et du secteur privé. Un nouvel acteur, le Commissariat à l'espace numérique et aux nouvelles technologies, devrait être créé et désigné comme le chef d'orchestre d'une partition nationale : une feuille de route définissant une organisation, un cadre réglementaire et financier et des objectifs dans les trois couches du cyberspace. Ce commissariat devrait préparer avec les milieux industriel et académique l'émergence, la maîtrise et la pérennité des facteurs clés nationaux et européens d'une souveraineté 2.0 pour préparer la prochaine étape de la révolution numérique en marche. Au-delà de cette première approche globale et face à la grammaire propre du cyberspace, la question du développement, de la réalisation et de la maîtrise de tous les éléments constitutifs d'un *Intranet* national sécurisé et résilient devrait également être posée à court terme.

(32) Par extension du périmètre du Décret n° 2014-479 du 14 mai 2014 relatif aux investissements étrangers soumis à autorisation préalable.

Le cyberspace, nouvel espace de souveraineté à conquérir

Éléments de bibliographie

- ANSSI, *Défense et de sécurité des systèmes d'information : stratégie de la France*, février 2011, 24 pages (www.ssi.gouv.fr/).
- BELLANGER Pierre, *La souveraineté numérique*, Stock, 2014, 264 pages.
- BOCKEL Jean-Marie, *La cyberdéfense : un enjeu mondial, une priorité nationale (Rapport d'information n° 681)* ; Commission des affaires étrangères, de la défense et des forces armées, Sénat, 18 juillet 2012, 158 pages (www.senat.fr/rap/r11-681/r11-681.html).
- COMMISSION DU LIVRE BLANC, *Livre blanc sur la Défense et la Sécurité nationale*, 2008, La Documentation française, 120 pages (http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf).
- DANET Didier et CATTARUZZA Amaël, *La Cyberdéfense – Quel territoire, quel droit ?*, Économica, 2014, 288 pages.
- DOSSÉ Stéphane, KEMPF Olivier et MALIS Christian, *Le Cyberspace : Nouveau domaine de la pensée stratégique*, Économica, 2013, 192 pages.
- DOUZET Frédéric, « Cyberspace : enjeux géopolitiques », *Hérodote* n° 152-153, Éditions La Découverte, 2014, p. 3-21 (www.herodote.org/spip.php?article616).
- HARREL Yannick, *La cyberstratégie russe*, Nuvis, 2013, 248 pages.
- HUYGHE François-Bernard, KEMPF Olivier et MAZZUCHI Nicolas, *Gagner les Cyberconflits – Au-delà du technique*, Économica, 2015, 176 pages.
- KEMPF Olivier, *Introduction à la cyberstratégie* (2^e édition), Économica, 2015, 240 pages.
- KEMPF Olivier, *Alliances et mésalliances dans le Cyberspace*, Économica, 2014, 192 pages.
- LIANG Quia et XIANGSUI Wang, *La guerre hors limite*, Rivages proches, 2006, 310 pages.
- LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity – Espionage, Strategy and Politics in the Digital Domain*, Oxford University Press, 2015, 400 pages.
- SCHMITT Michael N. (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.
- SGDSN, *Stratégie nationale pour la sécurité du numérique*, octobre 2015, 42 pages (www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf).
- SGDSN, *Livre blanc sur la Défense et la Sécurité nationale*, 2013, La Documentation française, 160 pages (www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf).
- VENTRE Daniel, *Chinese Cybersecurity and Defense*, ISTE Ltd and John Wiley and Sons Inc, 2014, 320 pages.

Entretiens :

- Professeure Frédéric Douzet, titulaire de la Chaire Castex de cyberstratégie de l'IHEDN, professeure à l'Institut français de géopolitique de l'Université Paris 8.
- Alix Desforges, chercheuse à la Chaire Castex de cyberstratégie, doctorante à l'Institut français de géopolitique de l'Université Paris 8.
- Aude Géry, chercheuse à la Chaire Castex de Cyberstratégie.
- Marc Hecker, docteur en science politique de l'Université Paris 1 Panthéon-Sorbonne, chercheur au Centre des études de sécurité de l'Ifri (Institut français des relations internationales), directeur des publications de l'Ifri et rédacteur en chef de *Politique étrangère*.
- Arnaud Kalika, responsable « Sécurité et intelligence stratégique » du fonds d'investissement Meridiam, spécialiste de la Russie.
- Thierry Vandewalle, fondateur et gérant du fonds d'investissement Wind SRPL (investissements dans les secteurs d'Internet et des nouvelles technologies).

Révolution numérique : vers une armée numérique ?

Erwan ROLLAND

| Colonel (terre), auditeur de la 66^e session du CHEM.

Une révolution numérique en marche

Une révolution numérique encore en devenir

La croissance rapide des nouvelles technologies de l'information et de la communication (NTIC) et l'innovation dans les systèmes numériques sont à l'origine d'une révolution qui ouvre de nouvelles perspectives à la création du savoir et la diffusion de l'information, et qui bouleverse radicalement nos modes de pensée, de comportement, de communication et de travail. Cette révolution numérique ⁽¹⁾ peut ainsi se résumer par l'essor récent de l'informatique et d'*Internet*, et des mutations profondes qui se traduisent par une mise en réseau planétaire des individus, de nouvelles formes de communication (courriels, réseaux sociaux), une décentralisation dans la circulation des idées et de nouveaux modes de création de valeur et d'activités économiques.

Cette révolution numérique se caractérise par une véritable déferlante digitale qui, depuis l'apparition d'*Internet* dans les années 1990 et de l'*iPhone* en 2007, a fait surgir autant de nouveaux usages que de nouveaux acteurs imprévus (GAFAM : Google, Apple, Facebook, Amazon, Microsoft...) et plus agiles que l'*establishment* économique et institutionnel. Si la révolution numérique semble remettre fondamentalement en cause les règles actuelles du jeu économique, elle rend aussi plus flou un avenir encore mal cerné. Pour beaucoup d'acteurs économiques et institutionnels (défense, sécurité, éducation, formation professionnelle, administrations...) le mot d'ordre est donc de s'adapter rapidement avant d'être dépassé et de disparaître.

Cette révolution numérique à tout va se caractérise aussi par la dématérialisation (dont la démonétisation), la désintermédiation (ou ubérisation) et donc la disruption en perturbant le jeu des acteurs en place, les modes de vie et de fonctionnement qu'elle remplace ou élimine. Elle altère la structure et la nature même des différents secteurs d'activités économiques et étatiques régaliens et expose de ce fait les grands acteurs à la fois à de nouvelles menaces mais aussi de fabuleuses opportunités. Puisque le numérique rend perméable toutes les frontières, ses succès et ses contradictions touchent aussi bien la dimension internationale que le niveau le plus micro de la société et de la politique, dont les questions de sécurité et de défense ⁽²⁾.

(1) Définition de l'Union internationale des télécommunications (UIT).

(2) Conférence de l'Université de Montréal (Département de science politique), « Relations internationales : enjeu actuel, Politique du cyberspace », novembre 2016.

Révolution numérique :
vers une armée numérique ?

Les perspectives d'un futur supercalculateur quantique pouvant casser tous les systèmes de cryptage ou d'imprimantes 3D permettant à des groupes terroristes de réaliser des armes par fabrication additive ⁽³⁾ obligent les acteurs de la défense et de la sécurité nationale à conserver un temps d'avance et à évaluer les menaces possibles du futur pour mieux s'y préparer.

La défense et la sécurité ne sont bien évidemment pas épargnées

Si l'on s'appuie à la fois sur la loi de Moore ⁽⁴⁾ (qui a trait à l'évolution exponentielle de la puissance de calcul des ordinateurs) et sur la convergence des grandes révolutions technologiques à venir, l'impact potentiel sur l'ensemble de nos activités et plus encore sur les questions de sécurité et de défense est considérable. L'apparition de modes d'action novateurs permettant une atténuation de l'asymétrie des conflits peut effectivement avoir un effet disruptif conduisant à l'émergence de nouvelles stratégies de défense, de nouveaux modèles d'organisation militaire et de conduite des opérations. La convergence inéluctable des domaines relevant des Nanotechnologies, biotechnologies, de l'informatique et des sciences cognitives (NBIC) ouvriront très certainement la voie vers l'homme augmenté et seront également source de risques et d'opportunités dans le domaine militaire. Des exemples tirés de l'actualité récente témoignent des grandes ruptures technologiques à venir et de leur impact immédiat sur les questions de sécurité et de défense.

Les drones, la robotisation et l'intelligence artificielle (IA). En janvier 2017 ⁽⁵⁾, le Pentagone annonçait avoir testé avec succès un essaim d'une centaine de petits drones *Perdrix*. Les progrès de l'IA rendent désormais possible la constitution de groupes de petits robots agissant collectivement pour remplir des missions coordonnées. Si certains drones sont détruits, l'ensemble continue à agir en se réorganisant. Lors de cet essai, les drones ont démontré qu'ils parvenaient à prendre des décisions collectives, adaptant ainsi leur comportement individuel aux aléas de la mission. Dessinés pour voler au moins par groupe de 20 ou plus, avec une mission bien définie à réaliser, les drones forment un organisme collectif, partageant un cerveau commun. Parce que chaque drone communique et collabore avec chacun de ses homologues, l'essaim n'a pas de *leader* et peut s'adapter au fur et à mesure si un nouveau drone rejoint le groupe ou si, au contraire, l'un est abattu.

Ces essais de drones, peu coûteux à fabriquer et tirant leur force de leur capacité à submerger par leur nombre les défenses de l'adversaire sont très certainement amenés à avoir un bel avenir et illustrent parfaitement ce que les armées sont en droit d'attendre de la révolution numérique dans la conduite des opérations militaires (drones, robots, intelligence artificielle, connectivité...).

(3) Processus de fabrication qui transforme un modèle 3D en un objet physique, en assemblant des couches successives d'un même matériau.

(4) Gordon E. MOORE, « Cramming More Components onto Integrated Circuits », *Electronics*, vol. 38 n° 8, 19 avril 1965, republié ensuite dans *Proceedings of the IEEE*, vol. 86 n° 1, janvier 1998 (www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf).

(5) Tiré d'un article d'Anne BAUER s'appuyant sur le communiqué du service des capacités stratégiques (SCO) du Pentagone : « Défense : le Pentagone teste des "essaims" de drones », *Les Échos*, 12 janvier 2017 (www.lesechos.fr/).

Dans le registre des télécommunications, le projet américain de Greg Wyler (ancien ingénieur de Google, à la tête de la société OneWeb) de lancer à horizon 2019 plusieurs centaines de satellites (900 satellites pesant moins de 150 kg contre 5 tonnes pour les satellites de télécoms actuels) en orbite basse pour fournir un accès à *Internet* préfigure également une autre révolution à venir en matière d'accès à *Internet* et d'augmentation des débits. D'autres projets d'*Internet* par l'Espace pourraient également voir le jour, notamment avec Elon Musk (créateur de Paypal, actuel PDG de Tesla et de Space X, société qui envoie déjà des fusées pour la NASA) qui envisage, avec le soutien financier de Google, d'envoyer 4 000 petits satellites et de les interconnecter avec des rayons laser.

Le Big et Fast Data et l'Internet des objets (IdO). L'explosion quantitative de la donnée numérique contraint à de nouveaux ordres de grandeur qui concernent la capture, le stockage, la recherche, le partage, l'analyse et la visualisation des données. Les prochaines guerres seront très certainement en partie remportées par ceux qui seront en mesure de mieux contrôler, analyser, exploiter, protéger et attaquer une somme de plus en plus importante d'information. À l'instar du *cloud* civil, l'ensemble des vecteurs, effecteurs et structures de commandement connectés fera appel au *cloud* militaire (ou *combat cloud*) qui réduira la ségrégation naturelle entre chaque milieu (terrestre, maritime, aérien et Espace) et qui permettra de compresser et d'accélérer la boucle décisionnelle (boucle Observation, orientation, décision, action – OODA) et le cycle de ciblage.

Le *Big et Fast Data* et la géodistribution (répartition des ressources disponibles entre des *data centers* ⁽⁶⁾ centralisés, décentralisés et jusque dans les terminaux mêmes des utilisateurs) vont considérablement faire évoluer le *cloud computing* ⁽⁷⁾ et donc le *combat cloud* à horizon 2030. Selon certaines estimations, 40 zétaoctets de données (40 000 milliards de gigaoctets) seront créés à horizon 2020, en grande partie générés par les 30 Mds d'objets connectés (informations provenant des messages envoyés, vidéos publiées, informations climatiques, signaux GPS, enregistrements transactionnels d'achats en ligne...). Le volume de données qui sera généré dans le secteur de la défense (ne serait-ce qu'au travers de la fonction Intelligence, surveillance et reconnaissance, *ISR*) sera tout aussi exponentiel dans les années à venir. L'essor des applications tirant parti en flux tendu de ces données exigera des traitements extrêmement rapides et donc au plus près des utilisateurs.

Ces évolutions numériques majeures ouvrent donc la voie à un environnement pervasif et ubiquitaire, et un monde dans lequel les objets et les individus pourront communiquer et se localiser à tout moment avec les autres éléments, quel que soit leur « milieu de rattachement » (terrestre, aérien, maritime et espace). Les enjeux liés au

(6) Un centre de données est un site physique sur lequel se trouvent regroupés des équipements constituant le système d'information (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications...).

(7) Selon le *National Institute of Standards and Technology (NIST)*, le *cloud computing* se définit comme le modèle informatique qui permet un accès pratique et à la demande, par le réseau, à un ensemble partagé de ressources informatiques configurables (serveurs, stockage, applications et services) qui peuvent être rapidement provisionnées et mises à disposition avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de service.

combat cloud, c'est-à-dire à la maîtrise et à la gestion des données (transport, stockage, *management*, analyse, sécurisation, disponibilité...) sont ainsi au cœur des défis à relever.

Le cyberspace, nouvel espace de confrontation

Le Cyberspace, un milieu à part entière, fédérateur des autres milieux

Le cyberspace est une métaphore souvent utilisée pour rendre plus facilement compréhensible l'expansion rapide des technologies numériques et la place qu'elles occupent désormais dans nos vies.

Le cyberspace (défini par l'Agence nationale pour la sécurité des systèmes d'information, ANSSI comme « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques ») est donc tout naturellement un espace de compétition et de confrontation pour l'ensemble des activités qui sont nées et vont naître de la révolution numérique. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme, criminalité et sabotage trouvent dans le cyberspace un nouveau champ d'expression.

Le cyberspace s'articule autour de trois couches : **la couche physique** qui comprend les éléments matériels et les éléments actifs (câbles sous-marins, fibres optiques, satellites, serveurs, routeurs, ordinateurs...), **la couche logicielle ou applicative** (systèmes d'exploitations, logiciels, protocoles...) – qui concentre près de 80 % des attaques informatiques –, et **la couche sémantique** de l'information et des perceptions qui s'attache au sens contenu dans l'information.

Le cyberspace, comme l'environnement électromagnétique, supporte une quantité grandissante d'applications numériques civiles et militaires indispensables à de vastes pans d'activités économiques et régaliennes. Dans la sphère militaire, de nombreuses capacités opérationnelles reposent désormais en très grande partie sur l'usage et la maîtrise du cyberspace (et de l'environnement électromagnétique). Or, ce nouveau champ de confrontation se distingue par son caractère transverse aux autres milieux. Le cyberspace donne corps à un environnement pervasif et ubiquitaire. *De facto*, toute opération dans le champ du numérique doit donc viser à faciliter les opérations dans les autres environnements opérationnels (terrestre, maritime, aérien et Espace).

Dans ce nouvel espace de confrontation, la supériorité opérationnelle ne pourra être obtenue qu'à condition de s'approprier les *game-changers* technologiques de la révolution numérique (robotique, IA, cyber, fabrication additive, IdO, *Big* et *Fast Data*...) et de faciliter la coopération de l'ensemble des acteurs prenant part au combat et au règlement d'une crise.

Ces *game-changers* technologiques offriront à terme des capacités de compréhension et de modélisation de l'environnement des opérations militaires. Ils donneront la possibilité pour le chef militaire de faire face à la surprise, de réagir devant l'imprévu, d'influencer son adversaire en agissant sur les perceptions (au travers de véritables batailles narratives dans un champ informationnel qui va gagner en intensité), et donc de provoquer la surprise en se rendant imprévisible, grâce à ses propres capacités

d'adaptation. Les actions coordonnées dans le cyberspace démultiplieront l'efficacité des actions classiques dans les autres milieux.

Plus encore, la quantité d'information qui sera générée sur le champ de bataille, la puissance de calcul, les capacités de traitement informatique et les algorithmes prédictifs vont devenir le nerf de la guerre et les outils de modélisation-simulation-optimisation (MSO) ainsi que les modèles d'aide à la décision et à la compréhension ouvriront la voie à une nouvelle forme de guerre prédictive⁽⁸⁾. Dès lors, les synergies et la coordination étroite entre les acteurs du renseignement en amont, les différents échelons de commandement et les effecteurs dans chaque milieu seront au cœur des enjeux militaires à venir pour faire du cyberspace un véritable espace fédérateur des autres champs traditionnels de confrontation.

Le Cyberspace, une menace réelle, permanente et croissante

Quelques exemples récents illustrent les menaces réelles qui pèsent sur l'ensemble de nos secteurs d'activité : en décembre 2016, des *hackers* s'en prenaient ainsi au réseau de distribution électrique ukrainien, plongeant la moitié des foyers de la région d'Ivano-Frankivsk (1,4 million d'habitants au total) dans l'obscurité. L'année précédente, les autorités allemandes révélaient que de mystérieux pirates informatiques étaient parvenus à prendre le contrôle à distance d'un haut-fourneau, le poussant à une telle température que l'équipement industriel avait été irrémédiablement endommagé. La tentative de piratage, au printemps 2016 d'une centrale nucléaire allemande a fait grimper d'un cran les craintes des experts occidentaux en cybersécurité face à des commandos numériques difficiles à identifier avec exactitude. Cependant très souvent les regards se tournent vers Moscou, tout comme lors de la campagne présidentielle américaine où des *hackers* russes s'en seraient pris aux serveurs du comité national démocrate chargé de lever des fonds en faveur d'Hillary Clinton et sont ainsi soupçonnés d'avoir pu influencer les résultats des élections de la plus grande démocratie occidentale.

Ces incidents vont donc au-delà des simples actes de sabotage et visent à affirmer une forme de puissance et un pouvoir de nuisance susceptibles de peser dans des relations diplomatiques de plus en plus conflictuelles⁽⁹⁾.

Avec une hypothèse de 20 à 30 Mds d'objets connectés à horizon 2020 et l'apparition de nombreux acteurs (États, GAFAM, groupes terroristes, organisations intermédiaires de type *proxy*⁽¹⁰⁾, cybercriminels, hackers, mouvement cybermilitant de type Anonymous...), la menace cyber est donc plus que jamais devenue une réalité qui ne peut que s'intensifier, se diversifier et face à laquelle les armées et la France se sont déjà mises en ordre de marche.

(8) « Comment gagner une guerre perdue », conférence de Pierre BELLANGER, 31 décembre 2016.

(9) Propos recueillis par Baudouin ESCHAPASSE, *Le Point.fr*, 30 novembre 2016.

(10) Le terme de « *Proxy* » est à prendre au sens du rôle d'intermédiaire, en se plaçant entre deux hôtes pour faciliter ou surveiller des échanges.

Une réponse et une organisation complète qui devra évoluer face aux enjeux à venir

Déjà identifiés dans le *Livre blanc* de 2008, les menaces et les risques induits par l'expansion généralisée du cyberspace ont été confirmés dans celui de 2013. Une véritable dynamique existe au sein du ministère de la Défense (Mindef) autour des activités du numérique et du cyberspace. Un nombre important d'acteurs, d'organismes et de ressources a été créé et mis en place pour couvrir l'ensemble du périmètre lié au numérique et au cyberspace. Pour autant, le paysage semble parfois disséminé, voire compartimenté et segmenté.

Une organisation complète mais disséminée et compartimentée

Un **Officier général transformation digitale des Armées (OGTDA)** a été créé à l'automne 2016 à l'État-major des armées pour en accélérer la transformation digitale, préserver la supériorité face à un ennemi évoluant dans l'espace numérique et rechercher l'efficacité dans le domaine organique et fonctionnel, dans un contexte de ressources (financières et humaines) contraint.

Une **Direction [bicéphale] des systèmes d'information (DSI)** : à côté d'une **Direction générale des systèmes d'information et de communication (DGSIC)** ministérielle, davantage tournée vers la normalisation et la coordination interministérielle, la **Direction interarmées des réseaux d'infrastructure et des systèmes d'information (Dirisi)** est en lien étroit et constant avec l'ensemble des Armées, Directions et Services (ADS) qui réclament des systèmes d'information configurables, à la fois pour leurs activités fonctionnelles/métier (Systèmes d'information d'administration et de gestion – SIAG) mais aussi pour l'emploi opérationnel des forces (Systèmes d'information opérationnel et de commandement – SIOC).

Pour chaque ADS, l'enjeu des NTIC est véritablement la création de valeur et de nouveaux usages pour les différentes chaînes fonctionnelles (métiers). La notion de sécurité est primordiale, d'autant plus que les données sont convoitées et que les nouvelles façons de travailler (*cloud*, mobilité et nouveaux supports de type *smartphones/tablettes*) accentuent les risques. Véritable opérateur des systèmes d'information du Mindef, la Dirisi accompagne les ADS sur l'utilisation des nouvelles technologies, sur la gestion des risques et la notion de conformité légale de l'usage qu'ils en font. Dans la numérisation et la transformation du Mindef par les systèmes d'information et de communication (SIC), le rôle de la Dirisi prend une nouvelle dimension, en complémentarité de l'OGTDA.

La **Direction générale pour l'armement–Maîtrise de l'information (DGA-MI)** apporte au Mindef l'expertise technique dans les domaines des systèmes d'information et de communication, de la guerre électronique, les systèmes de missiles tactiques et stratégiques et du cyber.

Enfin pour compléter ce paysage ministériel, un **officier général Cyber** est en place depuis 2011, précurseur du **Commandement de cyberdéfense et des opérations cyber**. Le 12 décembre 2016, Jean-Yves Le Drian, alors ministre de la Défense, posait

en effet les bases d'une doctrine rénovée de la cyberdéfense et annonçait la création à l'été 2017 d'un commandement de la cyberdéfense. Récusant toute idée de dissuasion conventionnelle ou cyber, il a rattaché les problématiques cyber aux questions d'ordre conventionnel et a posé les bases de ce que pourraient être une doctrine et une stratégie cyber de la défense afin de mieux intégrer l'ensemble des volets cyber dans la pensée militaire.

Ainsi, **trois missions** principales sont assignées au domaine cyber. En premier lieu, le **renseignement** qui a pour objectif de contribuer à identifier nos failles et vulnérabilités, de détecter et caractériser les actions hostiles, d'en attribuer l'origine, de participer aux actions de remédiation et de contribuer à préparer les réponses offensives. En second lieu, la **Posture de Protection/Défense**, qui comprend la posture permanente cyber (mesures réduisant les risques sur nos systèmes dont ceux des opérateurs d'infrastructures vitales), la défense en profondeur (ou cyber protection) et la défense de l'avant (ou lutte informatique défensive). Enfin, troisième mission, la **lutte informatique offensive** (entraver, neutraliser, riposter), qui doit permettre d'agir contre un ennemi cherchant à nuire à nos intérêts de sécurité et de défense.

La création d'un commandement de la cyberdéfense qui conforte les structures existantes et consolide les ressources allouées au sein du Mindef est-elle pour autant à la hauteur des enjeux à venir pour mener les opérations militaires dans l'espace numérique à horizon 2030 ?

Vers l'émergence d'une véritable armée numérique

Il existe encore de multiples acteurs qui agissent directement ou indirectement sur au moins l'une des trois couches du cyberspace et concourent à la fonction/communauté *C5ISR* (*Command, Control, Computer, Communications, Cyber, Intelligence, Surveillance, Reconnaissance*). Il y a historiquement et logiquement une dissémination et un cloisonnement (organisation en strates et en tuyaux d'orgue) entre l'ensemble de ces principaux « acteurs numériques » qui constituent le noyau dur de la fonction *C5ISR*, selon leur armée d'appartenance, leur milieu (terrestre, maritime, aérien, Espace) et niveau d'emploi (stratégique, opératif et tactique). États-majors opérationnels, management de l'information, data management, SIC, Cyber, guerre électronique (GE), gestion et exploitation du spectre électromagnétique, Renseignement d'origine électromagnétique (ROEM), Renseignement d'origine image (ROIM), Renseignement d'origine cyber (ROC), stratégie militaire d'influence et opérations d'information... sont autant de fonctions et d'acteurs dont l'action mérite d'être mieux coordonnée et intégrée pour favoriser les synergies.

Il appartient dès lors de traiter les « formes d'antagonismes » qui peuvent exister entre tous ces acteurs en adaptant l'organisation et les compétences pour lutter efficacement contre les enjeux de pouvoir et de territorialité qui peuvent prévaloir, à la fois entre les ADS mais aussi entre les niveaux stratégiques, opératifs et tactiques.

Une armée numérique, pour quoi faire ?

Le modèle actuel d'organisation de nos armées ne doit pas être un frein pour relever les défis de la révolution numérique. Garante d'une meilleure convergence et intégration de l'ensemble des capacités, la mise en place d'une véritable armée numérique doit offrir la faculté d'agir et de combattre conjointement pour relever un double défi : celui de la maîtrise d'une ressource humaine rare et convoitée et celui d'une meilleure efficacité opérationnelle.

Relever un enjeu RH majeur

Les transformations numériques actuelles et à venir suscitent de fortes attentes de profils hautement qualifiés et feront émerger de nouvelles compétences et de nouveaux métiers. *Chief data officer, data scientist, data protection officer, community manager, Web project manager, digital brand manager, chief data officer...* Pour ne citer que l'exemple du *Big et Fast Data*, le *data scientist* est chargé de « faire parler » les données et de les présenter sous un format simple. Le *data protection officer* est, quant à lui, garant de la protection des données sensibles au sein de son organisation. Autant de nouveaux métiers qui apparaissent en plus des métiers techniques liés aux NTIC elles-mêmes.

Pourtant, selon une étude Eurostat, 42 % des entreprises françaises rencontrent des difficultés pour recruter des spécialistes du numérique. La formation dans ces domaines est encore balbutiante et insuffisante. Le besoin des entreprises en *data scientists* est évalué entre 5 000 et 10 000 recrutements par an, alors que l'offre serait d'à peine 300 diplômés. De plus, les employeurs recherchent souvent une double compétence NTIC et métier (statistiques, mathématiques mais aussi développement, *marketing...*) ce qui rend le recrutement d'autant plus compliqué.

La défense n'échappe bien évidemment pas à cet enjeu majeur. Il est indispensable de bien appréhender les transformations en termes de RH qui découlent de la révolution numérique et du cyberspace pour se doter et mettre en œuvre les outils adéquats : modes de recrutement et rémunérations adaptés et capables de répondre à la concurrence, parcours professionnels attractifs (reconversion incluse) et favorables à la fidélisation du personnel (mobilité, validation des acquis et de l'expérience), équilibre entre les différentes catégories de personnel (civil et militaire), adaptation des statuts...

Plusieurs initiatives au sein du ministère de la Défense sont à relever dans ce domaine : le pôle d'excellence cyber, le réseau cyberdéfense de la réserve citoyenne, le projet d'Intelligence campus de la Direction du renseignement militaire (DRM) ou encore tout dernièrement la création d'un Brevet de technicien supérieur (BTS) cyber au Lycée militaire de Saint-Cyr-l'École. Autant d'initiatives qui préfigurent ce que pourrait être une véritable « École 42 de la défense », à l'instar de l'école française d'informatique privée créée par Xavier Niel (à l'origine de l'offre d'accès à *Internet* sous le nom de *Free* à la fin des années 1990), qui applique les principes de l'économie collaborative à l'éducation et à la formation.

Révolution numérique : vers une armée numérique ?

La création d'une armée numérique doit donc participer en tout premier lieu à cette volonté d'optimiser une ressource humaine tendue (parce que rare et sous-dimensionnée), volatile (parce que soumise aux évolutions technologiques rapides et incessantes) et très convoitée par un secteur privé plus rémunérateur. Anticiper les besoins en compétences, développer une gestion prévisionnelle des emplois, des effectifs et des compétences (GPEEC), recruter de nouveaux agents et fidéliser les meilleurs malgré la concurrence des entreprises privées, améliorer les rémunérations des agents non titulaires et des militaires sous contrat sont autant de défis RH à relever.

Garantir la supériorité opérationnelle

Comme le rappelle Jean-Yves Le Drian, « face à une attaque [cyber], il conviendrait que nous puissions proposer au président de la République un large éventail de réponses possibles, sans nous limiter par avance à la sphère militaire ni au domaine cyber »⁽¹¹⁾. La création d'une armée numérique doit donc également concourir directement à un double objectif : se doter d'une véritable capacité et liberté de manœuvre dans le cyberspace et être à même de mieux planifier et coordonner les actions dans le champ du numérique en appui de la manœuvre globale dans les autres environnements opérationnels en intégrant davantage les acteurs de la fonction *C5ISR*.

La numérisation offrira à terme les bénéfices escomptés à nos structures de commandement qui gagneront en agilité, en performance et en efficacité en surmontant le risque de saturation informationnelle. L'armée numérique de demain devra concourir à fluidifier le renseignement et le rendre plus accessible aux échelons opératifs et tactiques. Si les flux informationnels et numériques peuvent brouiller davantage la compréhension et l'appréciation de situation, l'automatisation du traitement des données et la croissance de la puissance de calcul permettront d'innover les forces et leurs effecteurs jusqu'au plus bas échelon pour répondre au besoin tactique d'immédiateté et de précision.

Pour conforter cette supériorité opérationnelle, cette construction *ab initio* d'un nouveau modèle d'armée numérique repose sur deux facteurs clés de succès : elle doit d'une part renforcer la performance des structures de commandement et d'autre part décloisonner et fluidifier les liens entre les acteurs du renseignement, les structures de commandement et les effecteurs.

Armée numérique vs armées numériques : quel format et quelle organisation ?

Il s'agit donc dès à présent de dessiner les contours d'un modèle d'intégration capable de tirer le meilleur parti des impacts à venir de la révolution numérique. S'appuyant à la fois sur l'axe d'intégration vertical (selon le niveau d'emploi : stratégique, opératif ou tactique) et horizontal (par milieu : terrestre, maritime, aérien et

(11) Jean-Yves LE DRIAN, « Déclaration du ministre de la Défense sur la cyberdéfense », Bruz, 12 décembre 2016 (<http://discours.vie-publique.fr/notices/163003632.html>).

Espace), l'armée numérique de 2030 devra donner corps à une fonction *C5ISR* structurée et cohérente.

C'est donc bien sur le degré d'intégration souhaité et réaliste que les trois scénarios qui suivent invitent à porter plus en avant la réflexion.

Scénario 1 : une armée numérique concentrée autour d'un acteur organique unique

À l'instar du modèle allemand mis sur pied au second semestre 2016 (création d'une composante et d'une direction générale *Cyber/Information domain*), la France pourrait prendre l'initiative de regrouper sous un commandement organique unique les principaux acteurs de la fonction *C5ISR* (SIC, cyber, ISR stratégique, ROEM et ROIM, stratégie militaire d'influence et opérations d'information, géographie selon le *benchmark* du modèle allemand).

Cette nouvelle structure aurait pour finalité première de décloisonner l'organisation en tuyaux d'orgue actuelle en concentrant plusieurs leviers d'actions aux mains d'une véritable autorité fonctionnelle unique du domaine *C5ISR* : doctrine, organisation, gestion des ressources (humaines : recrutement, plan de carrière, formation, réserve opérationnelle et citoyenne...) et financières (pouvoir adjudicateur), gestion de biens, préparation à l'engagement opérationnel pour les niveaux stratégiques et opératifs...

Une telle structure offrirait l'avantage de donner une compétence RH à ce nouvel acteur pour lui permettre de mieux coordonner les ADS. *A contrario*, les lignes de partage de responsabilités devront être clairement définies entre ce nouvel acteur, les ADS et la chaîne de conduite des opérations pour éviter de créer une technostructure sans âme ni conscience qui sépare et éloigne les acteurs numériques des armées.

Scénario 2 : une armée numérique concentrée autour d'un contrôleur opérationnel (OPCONer) interarmées unique

À l'instar du Commandement des opérations spéciales (COS), la France pourrait regrouper sous un commandement opérationnel interarmées unique l'ensemble des composantes *C5ISR* qui resteraient organiquement rattachées à leurs armées d'origine.

Ce modèle d'organisation concentré autour d'un *OPCONer* interarmées unique doit permettre d'accroître la performance du commandement et d'optimiser la coordination des opérations. Cette centralisation doit favoriser l'intelligence et l'appréciation de situation ainsi que l'accélération des processus décisionnels. Une action interarmées coordonnée et centralisée offre une meilleure garantie de conquérir la supériorité cybernétique et électromagnétique.

Une telle organisation offrirait au chef militaire en charge des opérations sur un théâtre la possibilité de disposer d'une articulation des moyens lui conférant une très grande agilité pour distribuer dans différents milieux des opérations variées dans des créneaux contraints.

**Scénario 3 : une armée numérique disséminée
autour de plusieurs acteurs « intégrables à la demande ».**

A contrario, le principe de subsidiarité entre les échelons stratégiques, opératifs et tactiques doit permettre d'éviter le piège d'une centralisation excessive et la saturation des échelons de commandement et de coordination.

Les *game-changers* de la révolution numérique doivent permettre d'envisager une déconcentration de l'organisation du commandement et de coordination des différents acteurs à l'échelon opératif et tactique. Un modèle déconcentré pourra offrir une plus grande réactivité à condition de mettre en place les structures de coordination *ad hoc* ⁽¹²⁾ permettant d'accroître la synergie des actions et optimiser les effets obtenus. Un tel modèle pourrait ainsi conduire à de véritables opérations distribuées, décentralisées dans la profondeur, avec une forme de commandement ubérisé de type *C to C* ⁽¹³⁾.

La contraction des délais décisionnels pour saisir les créneaux d'opportunité nécessite à la fois un bon niveau de délégation de l'échelon stratégique à l'échelon opérationnel, mais aussi un rapprochement d'exercice des responsabilités des niveaux opératifs et tactiques, et ponctuellement de privilégier une compression de ces deux niveaux hiérarchiques ⁽¹⁴⁾. Un modèle d'armées numériques déconcentrées au niveau des armées, selon une logique de milieux, devra donc reposer sur des structures de commandement opérationnel allégées et plus agiles, avec une empreinte au sol réduite et une mobilité accrue qui favoriseront l'appréciation de situation et la prise de décision en temps réel.

Chacun de ces trois scénarios reste bien évidemment modulable et peut faire l'objet de combinaisons et d'adaptations. Le premier modèle consistant à créer une autorité organique centralisée unique peut par exemple voir ce rôle dévolu à l'une des trois armées, dont les caractéristiques de milieu s'apparenteraient le plus à celles du cyberspace. Le troisième modèle décentralisé peut quant à lui se voir adjoindre la création d'une autorité fonctionnelle chargée de coordonner l'ensemble des acteurs déconcentrés pour faciliter leur intégration au cas par cas. Quant au second modèle, rien ne l'empêche d'évoluer dans le temps pour se rapprocher du modèle déconcentré au fur et à mesure que les ruptures technologiques faciliteront le principe de subsidiarité et la conduite d'opérations distribuées.

Conclusion

L'adaptation de notre outil de défense aux défis posés par la révolution numérique repose en partie sur l'analyse et la compréhension des courants ou signaux faibles

(12) Forme de plateau collaboratif pluridisciplinaire, comme c'est actuellement le cas pour coordonner avec précision les actions de la GE avec celles du ROEM et des SIC au travers de structures de type *Electronic Warfare Coordination Cell (EWCC)*, *SIGINT and Electronic Warfare Operation Center (SEWOC)*, ou encore *ElectroMagnetic Battlestaff (EMB)*.

(13) *Consumer to Consumer (C2C)* : est l'ensemble des échanges de biens et de services effectués directement entre deux ou plusieurs consommateurs. Dans le cas d'une opération militaire il s'agit donc de fluidifier les liens directs entre effecteurs sans transiter par un échelon de commandement/coordination intermédiaire.

(14) CICDE : *Les opérations contre un adversaire irrégulier Réflexion doctrinale interarmées RDIA-2011/004_ADIR(2011) N° 131/DEF/CICDE/NP* du 22 mai 2008, 2^e édition du 28 mars 2011 (www.cicde.defense.gouv.fr/).

Révolution numérique :
vers une armée numérique ?

qui sont annonciateur des grandes ruptures technologiques à venir. Il est important d'identifier dès à présent la fenêtre d'opportunité et de définir le rythme et la trajectoire de la transformation en profondeur qui amènera, le moment voulu, à la création d'une forme d'armée numérique dont le contour et le mode de fonctionnement restent à inventer.

Les germes de rupture résident souvent dans l'attentisme et une confiance excessive dans notre outil de défense. La préparation aux grandes ruptures à venir nécessite donc un effort permanent d'anticipation et d'imagination pour ne pas reproduire les schémas et les modes de pensée figés et surannés.

Pour relever efficacement les défis du numérique et affronter les menaces du cyberspace, il convient de cultiver notre résilience et notre capacité d'adaptation et de création au plan militaire. Quels que soient la forme choisie et le niveau d'intégration retenu, la mise sur pied d'une véritable armée numérique repose ainsi sur la capacité à faire davantage converger dès à présent l'ensemble des acteurs qui constituent la fonction *C5ISR*.

Cette armée numérique tirera le meilleur parti des ruptures technologiques à venir et créera les conditions pour transformer le cyberspace en cet environnement pervasif et ubiquitaire, fédérateur des autres champs traditionnels de confrontation. Elle favorisera la continuité entre les éléments techniques, organiques et opérationnels. Elle permettra de mieux combiner l'innovation technologique, stratégique et tactique et fera écho à Antoine de Saint-Exupéry qui disait : « pour ce qui est de l'avenir, il ne s'agit pas de le prévoir mais de le rendre possible ».

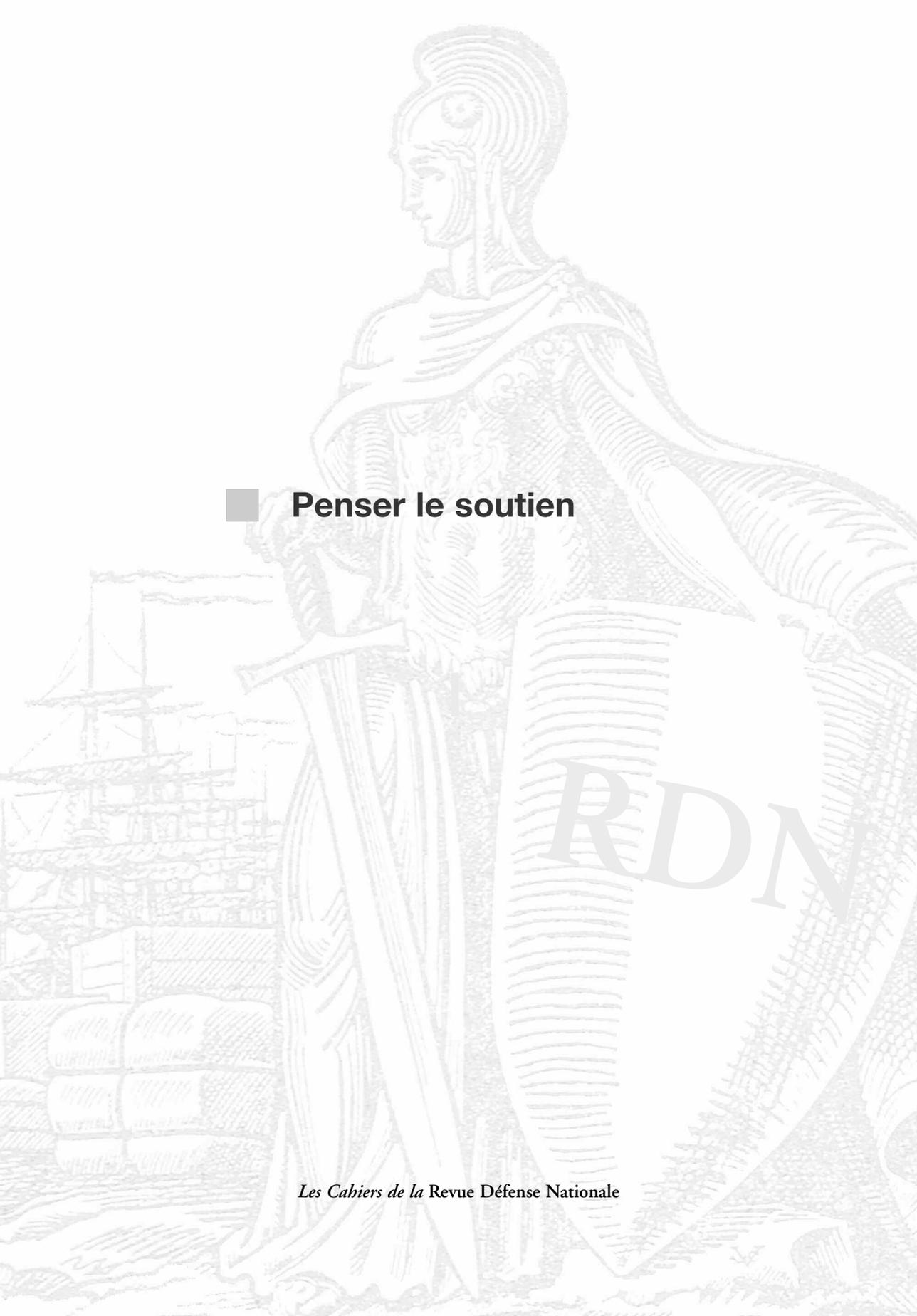
Révolution numérique : vers une armée numérique ?

Éléments de bibliographie

- ARMÉE DE TERRE : médiathèque « Action Terrestre Future : les facteurs de supériorité opérationnelle (FSO) » (www.defense.gouv.fr/terre/mediatheque/documentations).
- ANSSI, *Défense et de sécurité des systèmes d'information : stratégie de la France*, février 2011, 24 pages (www.ssi.gouv.fr/).
- BELLANGER Pierre, *La souveraineté numérique*, Stock, 2014, 264 pages.
- BOCKEL Jean-Marie, *La cyberdéfense : un enjeu mondial, une priorité nationale (Rapport d'information n° 681)* ; Commission des affaires étrangères, de la défense et des forces armées, Sénat, 18 juillet 2012, 158 pages (www.senat.fr/rap/r11-681/r11-681.html).
- BRYANT William D., *International Conflict and Cyber superiority: Theory and Practice*, Routledge, 2015, 250 pages.
- COMMISSION DU LIVRE BLANC, *Livre blanc sur la Défense et la Sécurité nationale*, 2008, La Documentation française, 120 pages (http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf).
- Dossier « Mars et Vulcain. Technologie et art de la guerre », *Histoire & Stratégie* n° 12, octobre-décembre 2012.
- NYE JR Joseph S., « Nuclear Lessons for Cyber Security? », *Strategic Studies Quarterly*, vol. 5 n° 4, Hiver 2011, p. 18-38 (www.au.af.mil/au/ssq/2011/winter/nye.pdf).
- SGDSN, *Livre blanc sur la Défense et la Sécurité nationale*, 2013, La Documentation française, 160 pages (www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf).
- SGDSN, *Stratégie nationale pour la sécurité du numérique*, octobre 2015, 42 pages (www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf).

Entretiens

- Général de division aérienne Bruno MAURICE, Officier général transformation digitale des armées (OGTDA).
- Professeure Frédérick DOUZET, titulaire de la Chaire Castex de Cyberstratégie.
- Colonel Olivier KEMPF, Officier Cyberdéfense et transformation digitale, division plan et programmes, État-major de l'Armée de terre (EMAT).
- Colonel (R) Olivier BERTRAND, Chargé de mission *Smart Base*, Centre études réserves partenariats de l'Armée de l'air (Cerpa).
- Capitaine de vaisseau Bertrand DU LESELLIER DU CHEZELLE, officier de cohérence opérationnelle à la division cohérence capacitaire de l'EMA et l'ingénieur de l'armement Frédéric BOUYER, architecte de préparation des systèmes *C4ISR*, DGA.
- Capitaine de vaisseau Laurent CELERIER, Comcyber.
- Lieutenant-colonel Pierre-Arnaud BORRELLY, EMA/SCOPS/Cyber.
- Lieutenant-colonel Jérôme DE LESPINOIS, chargé d'étude DGRIS/Irsem.
- Laurent TARD, Défense et sécurité, Directeur offre simulation, SOPRA-STERIA.



■ **Penser le soutien**

RDN

La loi d'Augustine est-elle une fatalité pour les armées françaises à 10 ans ?

Damien WALLAERT

| Colonel (terre), auditeur de la 66^e session du CHEMA.

Un lien fort entre équipement moderne, technologie et coût

Une dynamique de hausse des coûts difficile à freiner

De nombreux auteurs et experts ont théorisé la hausse inexorable des coûts des équipements militaires et la baisse en conséquence des formats des armées considérées. Le plus célèbre d'entre eux est Norman R. Augustine, ancien sous-secrétaire d'État pour l'*US Army* au Pentagone de 1975 à 1977 et président de Lockheed Martin à la fin des années 1990. Il a élaboré notamment une loi (n° 16) selon laquelle : « Si les méthodes du Pentagone et l'évolution des coûts ne changent pas, le budget du Pentagone autour de 2050 servira à acheter un seul avion tactique. Celui-ci sera confié trois jours par semaine à l'*US Air Force*, trois jours à la *Navy* et le septième au *Marine Corps*.⁽¹⁾ » Norman R. Augustine, 1978.

Un expert américain des acquisitions d'équipements militaire du Pentagone a prolongé les courbes d'Augustine au regard des programmes en cours ou futurs (*F-22*, *F-35* pour l'*USAF*, *CVN-21* pour l'*US Navy*...) et conclut à une vérification de cette tendance, menant pour lui à une « banqueroute » programmée⁽²⁾ de la défense américaine. À titre d'exemple, la dérive budgétaire du *F-35* est de 77 % du coût initial, celle du *F-22* de 386 % et ce programme a été stoppé après 187 avions construits sur les 780 prévus.

La dynamique exprimée dans cette loi semble malheureusement se vérifier pour de nombreux équipements et dimensionner les parcs de nos armées occidentales dans une large mesure⁽³⁾. Les systèmes associés suivent malheureusement la même tendance : le système de guidage d'un missile air-air comptait pour 10 à 20 % du prix du missile il y a quelques années quand il compte pour plus de 50 % aujourd'hui⁽⁴⁾.

(1) Norman R. AUGUSTINE, *Augustine's Laws*, American Institute of Aeronautics, Inc, New York, 1982.

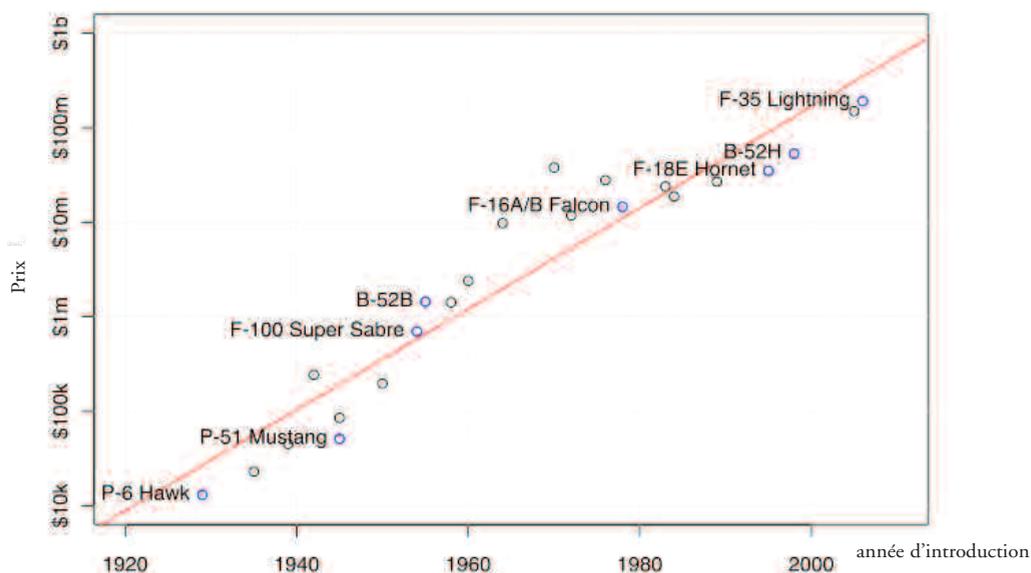
(2) John D. CHRISTIE, « DOD on a Glide Path to Bankruptcy », *Proceedings Magazine*, vol. 134/6/1,264, juin 2008, US Naval Institute.

(3) Jérôme DE L'ESPINOIS, « La puissance aérienne a atteint sa maturité, pas son déclin », *Guerre & Histoire* n° 4, p. 97, décembre 2011 citant Martin VAN CREVELD, *The Age of Air Power*, Public Affairs, New York, 2011.

(4) Scott O'NEIL, « A New Approach to Tactical Weapon Systems », *Proceedings Magazine*, vol. 142/2/1,356, février 2016, US Naval Institute.

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

Courbe d'Augustine ⁽⁵⁾ : prix des avions de combat américains



S'il est toujours délicat de comparer des chiffres qui ne couvrent pas les mêmes périmètres, le tableau suivant confirme clairement une tendance lourde d'augmentation des coûts des matériels militaires français.

Comparaison intergénérationnelle à l'achat ⁽⁶⁾ (coût unitaire en euros constant)

Matériel précédent	Coût d'achat	Matériel nouveau	Coût d'achat
Char <i>AMX-30</i>	1-2 M €	Char <i>Leclerc</i>	10,2 M €
VTT <i>AMX-10P</i>	1-2 M €	<i>VBCI (Véhicule blindé de combat d'infanterie)</i>	3,7 M €
Porte-avions <i>Charles-de-Gaulle (CDG)</i>	3 Mds €	2 nd porte-avions ?	3,2 Mds €
Hélicoptère <i>Gazelle HAP</i>	25,5 M €	Hélicoptère <i>Tigre</i>	35,5 M €
Hélicoptère transport	24,7 M €	Hélicoptère <i>NH90</i>	30 M €
<i>Mirage 2000</i> monoplace	9,4 M €	<i>Rafale</i> monoplace	142 M €
<i>C-130 Hercules</i>	53 M €	<i>A400M</i>	140 M €
Sous-marin nucléaire d'attaque (SNA) <i>Rubis</i>	182 M €	SNA <i>Barracuda</i>	1,45 Mds €
Frégate <i>La Fayette</i>	221 M €	Frégate <i>multimissions (Fremm)</i>	710 M €

(5) Graphique d'AUTOPILOT dans « Norman R. Augustine », *Wikipedia*, 7 janvier 2017.

(6) Sophie LEFEEZ, *Toujours plus chers, complexité des armements et inflation des coûts militaires*, Ifri-LRD, février 2013, citant des sources Cour des comptes, Assemblée nationale, ministère de la Défense, CPRA ; et Hugues ESQUERRE, *Quand les finances désarment la France*, *Économica*, p. 75, 2015. Pour les matériels de l'Armée de terre : dossier Grand rapport de l'Armée de terre 2016, référentiel des coûts 2016, p 53.

La loi d'Augustine est-elle une fatalité pour les armées françaises à 10 ans ?

Ceci s'accompagne inexorablement d'une diminution du volume des parcs. Entre 1990 et 2010, on a pu constater la division par deux du parc d'avions de combat et d'hélicoptères (Aviation légère de l'Armée de terre – Alat – et Armée de l'air) tandis que l'Armée de terre est passée de près de 800 chars de bataille à 200 *Leclerc*. De même, la Marine aura perdu près de la moitié de ses navires de combat entre 1980 et 2020. La tendance restera la même avec le programme *Scorpion* pour l'Armée de terre qui remplacera par exemple 506 véhicules blindés actuels (256 *AMX-10RC*, 110 *ERC-90* et 140 *VAB HOT*) par 248 *Jaguar* ⁽⁷⁾. De même, 12 *A330 MRTT* (*Multi-role Tanker Transport*) remplaceront 14 avions ravitailleurs *KC-135* et les 5 avions de transport stratégiques ! À performance globalement équivalente des parcs grâce au progrès technologique, on constate donc de façon inexorable une diminution de leur volume.

De plus, on constate une croissance du coût de l'entretien des matériels :

Comparaison intergénérationnelle du budget d'Entretien programmé du matériel ou EPM ⁽⁸⁾ (ordre de grandeur)

Matériel ancien	Coût d'entretien annuel	Matériel nouveau	Coût d'entretien annuel
Hélicoptère <i>Gazelle</i>	1,5 M €	Hélicoptère <i>Tigre HAP</i>	15 M €
Hélicoptère <i>Puma</i>	4 M €	Hélicoptère <i>NH90 TTH</i>	10 M €
Avion <i>Super-Étendard modernisé (SEM)</i>	10 M €	Avion <i>Rafale Marine</i>	15 M €
Avion <i>Minage 2000</i>	5 M €	Avion <i>Rafale</i>	15 M €

Comme le disait un rapport du Sénat sur ce sujet en 2012, « si nous restons sur les mêmes logiques de recherche permanente des meilleures capacités technologiques pour l'ensemble de nos parcs et flottes, la contraction des formats va donc se poursuivre inexorablement » ⁽⁹⁾. De même, le coût en ressources humaines, s'il est difficile à quantifier précisément, ne peut qu'augmenter avec la technicité des matériels qui requièrent des qualifications de plus en plus grandes et souvent facilement transposables dans le secteur civil. La création de primes de technicité, dédiées à fidéliser des populations de techniciens rares est une illustration de ce surcoût induit.

Ceci a des conséquences claires sur le format des armées à budget constant et illustre la nécessité absolue, pour faire face à ce qui se vérifie de la loi d'Augustine, de faire progresser le budget français de la Défense dans les 10 ans.

La technologie, facteur de supériorité du stratégique au tactique : maîtrise de l'incertitude

Ce renchérissement des parcs a bien sûr des raisons objectives et sa justification opérationnelle. Il est en effet particulièrement complexe d'imaginer les guerres de demain, tant la conflictualité et les moyens d'action évoluent rapidement. Gaston

(7) Exemple cité par Nicolas MALDERA, *La mutation technologique de l'Armée de terre, le cas du programme Scorpion*, Ifrap, 20 juin 2016 (www.ifrap.org/).

(8) Sophie LEFEEZ, *op. cit.*, citant des sources du ministère de la Défense.

(9) COMMISSION DES AFFAIRES ÉTRANGÈRES ET DE LA DÉFENSE : *Forces armées : peut-on encore réduire un format « juste insuffisant » ? (Rapport d'information n° 680)*, 18 juillet 2012, Sénat, 66 pages (www.senat.fr/).

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

Bouthoul écrivait : « le perfectionnement des armes a été jusqu'à nos jours une garantie de survie en faveur des groupes capables de concevoir et d'utiliser une technique supérieure »⁽¹⁰⁾. Pourtant, pour le Chef d'état-major de l'Armée de terre (Cémat), « les récents engagements, en Afghanistan notamment, annonçaient la fin d'un cycle, celui de la suprématie des armées occidentales »⁽¹¹⁾.

Face à un ennemi mieux préparé, utilisant des technologies dites nivelantes, la recherche de la supériorité technologique restera un facteur-clé de notre puissance militaire. Contourner les stratégies de déni d'accès par des avions de plus en plus furtifs, crypter de plus en plus ses flux pour maintenir sa supériorité cybernétique, acquérir le renseignement le plus précis malgré les manœuvres de déception et éviter au maximum les dommages collatéraux seront des enjeux technologiques qui nécessiteront des investissements toujours conséquents et resteront une partie de l'équation militaire de demain. En outre, l'usage de la technologie sera souvent de réduire ce que Clausewitz appelle le « brouillard de la guerre »⁽¹²⁾, autrement dit l'incertitude. Comme le disait Donald Rumsfeld, alors secrétaire à la Défense américain en 2002, « notre défi dans ce nouveau siècle est difficile : défendre notre Nation contre l'inconnu, l'incertain, l'invisible et l'inattendu »⁽¹³⁾.

L'émergence de la fonction « connaissance-anticipation » dans le *Livre blanc sur la Défense et la Sécurité nationale* de 2008 a souligné l'importance (et la sous-estimation passée) des moyens techniques dédiés au renseignement stratégique qui permettront d'anticiper les crises et de mieux cerner les enjeux de sécurité. Au niveau opératif, les moyens de commandement (*Command and control*), de renseignement (*ISR*) ou de projection de puissance participeront à la supériorité de la Force déployée sur un ennemi asymétrique. La surveillance du champ de bataille par des drones *Reaper* de la force *Barkhane* et leur armement inéluctable à moyen terme sont un facteur indéniable de supériorité sur l'ennemi. Même s'il adapte ses comportements à cette menace, il n'est pas encore capable de s'y soustraire totalement.

Le niveau tactique reste le champ d'action privilégié de la supériorité technique. Elle peut s'y exprimer pleinement et donner ponctuellement l'ascendant, en milieu ouvert de type sahélien ou en zone urbaine. En outre, la notion de duel, qui reste intrinsèque au combat, privilégie également la recherche de la supériorité technologique : « pourquoi le *Leclerc*, pourquoi le *Tigre* ? C'est oublier que les grandes mutations stratégiques ne modifient pas les conditions du duel des unités »⁽¹⁴⁾.

(10) Gaston BOUTHOU, *Traité de polémologie*, Payot, 1970, p. 142, cité par Jérôme DE L'ESPINOIS dans son article « L'usage de la puissance aérienne contre les formes irrégulières de la guerre » in Hew STRACHAN, Christian MALIS et Didier DANET, *La guerre irrégulière*, Économica, 2011, p. 329.

(11) Général Jean-Pierre BOSSER (Cémat), préface d'*Action terrestre future*, septembre 2016, p. 2.

(12) Carl VON CLAUSEWITZ, *De la guerre* (présenté par Gérard Chaliand), Perrin, 2014, 448 pages.

(13) Donald RUMSFELD, « 21st Century Transformation of the US Armed Forces », cité par Renaud BELLAIS dans « Technology and the Defense Industry: Real Threats, bad Habits, or New (Market) Opportunities? », *Journal of Innovation Economics & Management*, vol. 2 n° 12, 2013, p. 71.

(14) Général Bernard BARRERA, « France : opérations récentes, enjeux futurs », *Res Militaris*, décembre 2016, citant le général Yves CRÈNE, « Audace et raison : vers la consolidation d'une Armée de terre renforcée », *Défense nationale & Sécurité collective* n° 621 juin 2000, p. 11-23.

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

Il ne faut pas sous-estimer non plus l'impact de la technologie sur le moral du combattant. Conscient de l'effort de la Nation pour sa protection ou son efficacité opérationnelle, il n'en est que plus motivé et prêt à remplir sa mission, confiant dans son matériel et sûr d'un ascendant sur l'ennemi.

Les armées occidentales sont également confrontées à l'exigence de rester en phase avec les évolutions technologiques voire aux ruptures à venir : hyper-vélocité, armes à effet dirigé, réalité augmentée, Internet mobile, intelligence artificielle, nano-technologie, impression 3D, machines auto-apprenantes, physique quantique (rupture des cryptages, radar anti-furtivité...). La défense française ne peut faire autrement que d'intégrer les technologies émergentes – *a minima* dans les systèmes existants – sous peine de déclassement et de risque de contournement technologique.

Une exigence de protection du combattant qui restera très forte

L'enjeu de la protection du combattant est avant tout politique dans une démocratie. C'est le chef des armées – le président de la République – qui rend compte à la Nation de la vie de ses soldats et de leur sacrifice. Il est donc prévisible que la protection des combattants restera une priorité dans la conception des programmes d'armements de demain et donc un facteur de surcoût. Le programme *Scorpion* de l'Armée de terre est à cet égard édifiant. Cet impératif a pu participer à la décision de ne pas acheter un modèle existant chez Nexter comme le *Titus* pour remplacer le véhicule de base de l'infanterie française future mais demander la conception d'un engin plus robuste et mieux protégé que sera le *Griffon*. Malgré la volonté opérationnelle de « sahélier »⁽¹⁵⁾ les forces pour les rendre plus agiles, plus aptes à contrer un ennemi sur *pick-up* et se fondant dans le terrain, l'impératif de protection s'imposera et continuera d'expliquer en partie les coûts importants des nouveaux matériels.

Une BITD fragile, enjeu de souveraineté vs critères objectifs de rentabilité économique

Il convient de ne pas sous-estimer l'importance de l'industrie de défense pour une puissance militaire. La Russie, la France, les États-Unis, la Grande-Bretagne ou l'Allemagne prennent cette variable en compte dans leur équation globale de puissance. Les pays émergents (Brésil, Inde, Chine) cherchent également à développer leur industrie de défense, jugée essentielle à leur souveraineté. Ceci peut se faire d'ailleurs parfois au détour de contrats de type *Rafale* avantageux en termes de transfert de technologie.

La France ne déroge pas à cette règle parfois même érigée en dogme. La Base industrielle et technologique de défense (BITD) française représente 20 Mds € de chiffre d'affaires, 165 000 emplois souvent de haute technicité et faiblement délocalisables, 20 grands groupes, 4 000 entreprises dont 400 jugées stratégiques. Cette autonomie industrielle, notamment pour toute la chaîne de la dissuasion nucléaire, se traduit par un soutien à ces entreprises et parfois par des choix de programmes dont l'objectif est directement ou indirectement le maintien d'une activité suffisante à ces

(15) Général Xavier DE WOILLEMONT (*Comanfor Barkhane*), cité par Alain BARLUET, « Opération "Barkhane" : le soutien indispensable du puissant allié américain », *Le Figaro*, 8 mars 2017.

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

entreprises ou bureaux d'études jugés stratégiques ⁽¹⁶⁾. De plus, l'industrie de défense, par nature politique, est dépendante de commandes publiques (pour une part de moins en moins forte il est vrai). Cette inversion possible de la loi de l'offre et de la demande peut contribuer, si on cumule cet aspect au besoin de concentration des acteurs pour plus de souveraineté, à une structure de marché atypique et génératrice de surcoûts. Cela peut en effet créer des situations de dépendances mutuelles et de monopoles sectoriels qui faussent la concurrence. DCNS (Naval Group désormais) est par exemple le seul constructeur de navires de guerre français comme Nexter est seul sur de nombreux segments des besoins de l'Armée de terre.

De plus, l'investissement de l'État en matière de R&D peut être jugé très important (700 M € par an consacrés aux études amont avec un objectif à 1 Md). Le budget de R&D représente entre 10 et 20 % du chiffre d'affaires des 10 plus grands groupes industriels français et 20 000 emplois dans les bureaux d'études ⁽¹⁷⁾. Ce qui compte est la destination de ces études et on peut toujours se demander si « un tel contexte n'a pas nourri un environnement industriel dans lequel les entreprises sont encouragées à promouvoir les technologies avancées plutôt que de chercher à minimiser le coût des équipements » ⁽¹⁸⁾. En d'autres termes, on pourrait parler d'une motivation industrielle structurelle à privilégier des stratégies de *high-tech*.

Le progrès technologique, un démultiplicateur de puissance indéniable

Le progrès technologique permet de limiter les volumes de certains équipements pour un même effet militaire. Une *Fremm* aujourd'hui a une puissance multidimensionnelle décuplée par rapport à une frégate d'ancienne génération. Un char *Leclerc*, avec sa capacité de tir en roulant, son chargement automatique, sa mobilité, son système de navigation et son canon de 120 millimètres a la capacité de combat d'un peloton d'*AMX-30B2*. La mobilité et la puissance de ces vecteurs permettent en outre de compenser en partie leur plus faible nombre par la capacité à basculer l'effort et la zone couverte par les nouveaux capteurs. De même dans l'*US Air Force*, le couple avion furtif *F-117/F-111H* et arme guidée laser s'est révélé 13 fois plus destructeur qu'autant de *F-111* utilisant des armes non guidées lors de la guerre du Golfe en 1991 ⁽¹⁹⁾. Un raid aérien américain contre la Libye en 1986 mobilisait 77 avions et deux groupes aéronavals quand une opération similaire en 2017 n'engageait que 17 avions et des drones ⁽²⁰⁾.

La notion de rapport de force a donc tendance, si l'on n'y prend pas garde, et pour des raisons objectives décrites ci-dessus, à s'effacer devant celle de rapport de

(16) Caroline SALAHUN, « Recherche et technologie de défense : l'avenir se prépare aujourd'hui », *RDN* n° 769, avril 2014, p. 111-115.

(17) *Livre blanc sur la Défense et la Sécurité nationale*, 2008, p. 262.

(18) Renaud BELLAIS, « Technology and the Defense Industry: Real Threats, bad Habits, or New (Market) Opportunities? », *op. cit.*

(19) Jérôme DE L'ESPINOIS, *Guerre & Histoire*, *op. cit.*, p. 96.

(20) David DEPTULA, « Long Range Strike: 'More Potent', More Survivable & Cheaper », *Breaking Defense*, 31 janvier 2017 (<http://breakingdefense.com/2017/01/long-range-strike-more-potent-more-survivable-cheaper/>).

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

puissance, c'est-à-dire une somme d'effecteurs. Pourtant, on verra que gagner une guerre met en œuvre d'autres facteurs que ceux de la simple puissance technologique.

L'exemple américain de la complexité de l'équation

Une lecture très rapide de l'histoire militaire américaine depuis la Seconde Guerre mondiale peut illustrer la difficulté à trouver l'équilibre entre deux écoles structurantes de la pensée militaire : celle de Jomini, optimiste, statistique, offensive, susceptible d'orienter vers le technologisme et celle de Clausewitz, pessimiste, réaliste, défensive allant davantage vers la masse. D'un Eisenhower rassemblant des troupes en Angleterre avant de débarquer avec une masse critique le 6 juin 1944, à un MacNamara, venant de l'industrie automobile et appréhendant le conflit au Vietnam comme une équation mathématique (*body count*), l'armée américaine a connu deux approches différentes. La fin de la guerre du Vietnam a d'ailleurs vu le retour de la masse avec plus de 500 000 GI's mais malheureusement trop tardivement. Les années 1970 à 1990 connaîtront une approche plus massive qui trouvera son apothéose en 1991 lors de la reprise du Koweït par le général Schwarzkopf qui refuse de déboucher avant d'avoir 500 000 hommes ⁽²¹⁾ malgré une très forte pression de Washington.

Le reflux se fera au bénéfice des dividendes de la paix et de la croyance au tout technologique sous l'influence des néoconservateurs comme Donald Rumsfeld, Paul Wolfowitz ou Dick Cheney. Outre leur appui à la fameuse *Revolution of Military Affairs* (RMA), ils prôneront l'intervention limitée en appui de troupes locales en Afghanistan en 2001-2002, portée par le couple forces spéciales/missiles de croisières. Ils réitéreront en 2003 par une intervention en Irak dont ils limiteront le volume à 130 000 hommes contre l'avis des militaires, ce qui a donné le succès tactique mais le désastre stratégique que l'on sait. Cette alternance américaine illustre la difficulté à trouver le point d'équilibre entre les modèles d'armée et la place de la technologie.

Maîtriser les effets de la loi d'Augustine : possibilité et nécessité

Un retour d'expérience qui s'impose : garder des formats seuils pour faire masse

La réflexion autour des conséquences de la loi d'Augustine sur les armées à 10 ans revient à poser la question de l'existence de seuils en deçà desquels les armées françaises, pour conserver la capacité d'assumer leurs contrats opérationnels, notamment de souveraineté nationale, ne devront pas faire descendre leur volume de plate-formes (véhicules, blindés, canons, drones, hélicoptères, navires...).

Or, il se confirme que la masse est une vertu militaire et un facteur de puissance, notamment sur le temps long, celui des opérations. Le général de Villiers, Chef d'état-major des armées (Céma) de 2014 à 2017, l'a rappelé dans une tribune le 20 décembre 2016, pour faire face aux contrats opérationnels du *Livre blanc* de 2013, déjà largement dépassés : la situation « n'est pas tenable dans un contexte de dégradation durable de la sécurité et ne pourra être résolue par une réponse exclusivement

(21) Général H. Norman SCHWARZKOPF, *Mémoires* (avec la collaboration de Peter Petre) Plon, 1992, 573 pages.

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

fondée sur le “tout-technologique” »⁽²²⁾. Cette notion est reprise dans les documents de travail de l'État-major des armées (EMA) qui précise que l'ascendant sera pris sur l'ennemi par le nombre et la technologie. L'Armée de terre, dans *Action terrestre future*, ne dit pas autre chose : gagner la guerre, fut-elle hybride, restera la capacité à vaincre l'ennemi mais également à contrôler durablement le milieu dans laquelle il évoluait pour lui en empêcher la disposition⁽²³⁾. Ce contrôle sera possible par l'utilisation de capteurs et d'effecteurs, robotisés ou non, mais en nombre suffisant. Le milieu d'évolution de l'ennemi étant vraisemblablement destiné à être urbain et au sein des populations, la présence humaine armant des plateformes nombreuses restera un gage d'efficacité dans la gestion durable des conflits. L'emploi de la masse comme facteur de supériorité opérationnelle laisse donc apparaître la notion de seuil critique capacitaire en dessous duquel les forces armées ne doivent pas descendre sous peine d'être incapable de changer le sens de la guerre et pas seulement de la bataille.

D'autres voies existent pour imposer sa volonté militairement

La puissance militaire ne réside pas que dans la technicité de ses parcs d'armement mais dans la notion plus englobante de capacité⁽²⁴⁾. De plus, la force morale, la volonté politique, comme celle qui a permis la surprise et la réussite de *Serval* en janvier 2013, l'expérience des combattants, la standardisation des procédures permettant notamment une coopération interarmées, la capacité physique, technique et surtout intellectuelle à manœuvrer, à créer des rapports de force, à choisir un effet majeur sur le terrain ou sur l'ennemi, la capacité à influencer dans tous les milieux sont de véritables facteurs de puissance militaire, parfois peu dépendants de la technologie. L'opération *Sangaris* en Centrafrique de 2013 à 2016 a été à ce titre illustrative. Ces facteurs, malgré l'apparition et l'intégration nécessaires de nouvelles capacités, restent des atouts non négligeables en vue d'une victoire en particulier si l'on lui souhaite des effets durables.

Mettre en réseau des systèmes alliant très haute technologie et nombre importants de vecteurs moins sophistiqués

La supériorité militaire sera soutenable si elle permet la connexion, la mise en réseau d'effecteurs, humains ou techniques pour obtenir un effet donné sur le terrain. On peut imaginer certains vecteurs de très haute technologie mis en réseau avec des vecteurs moins onéreux mais plus nombreux, permettant de répondre aux deux besoins, celui de prise d'ascendant technologique et celui de masse de manœuvre, de saturation et de contrôle du milieu. Un *F-22* pourrait par exemple percer le « mur numérique » du type de celui que déploient les Syriens et les Russes (*S-300*, *S-400* et bientôt *S-500*) et ouvrir le chemin à des avions moins performants mais plus nombreux. Il les coordonnerait comme un *AWACS* (Système de détection et de

(22) Pierre DE VILLIERS (Céma), « Le prix de la paix, c'est l'effort de guerre », *Les Échos*, 20 décembre 2016 (www.lesechos.fr/idees-debats/cercle/0211613635015-le-prix-de-la-paix-cest-leffort-de-guerre-2051928.php).

(23) ÉTAT-MAJOR DE L'ARMÉE DE TERRE, *Action terrestre future : demain se gagne aujourd'hui*, 2016, p. 37-38 (www.defense.gouv.fr/actualites/communaute-defense/action-terrestre-future-demain-se-gagne-aujourd-hui).

(24) DORESE : Doctrine, organisation, ressources humaines, équipements, soutien, entraînement.

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

commandement aéroporté) en leur fusionnant la situation tactique ou en leur désignant des objectifs. Sous l'impulsion du sénateur McCain, l'*US Air Force* envisage par exemple l'acquisition de 300 avions de chasse à bas coût⁽²⁵⁾. L'Armée de l'air française est déjà sur cette voie en couplant en bande sahélo-saharienne un *Mirage 2000C*, doté d'un radar RDY, avec un *Mirage 2000D* non doté mais qui reçoit, *via* la liaison 16, toutes les données en temps réel collectée par le radar de son binôme ! Cette mise en réseau de deux vecteurs de technologie différente peut répondre à la nécessité de réduire les coûts. En l'occurrence, la DGA a renoncé, en vue de la rénovation à mi-vie du *Mirage 2000D* à installer ce radar.

Faire cohabiter des effecteurs de très haute technologie avec d'autres plus rustiques impliquera un emploi plus optimisé des effecteurs les plus onéreux. L'arrivée prochaine de l'*A400M Atlas* par exemple devra révolutionner le transport aérien militaire afin de faire donner à cet avion le meilleur de ses capacités. Plutôt que de faire des liaisons intra-théâtres en faible charge comme les *C-130*, il sera plus judicieux de le détacher peu de temps, lors des relèves par exemple, pour assécher les besoins en transport et de le faire venir de métropole (5 heures de vol entre Orléans et Niamey) pour des missions à haut rendement. Cela permettra de confier le reste des missions à d'autres vecteurs moins onéreux à l'heure de vol ou en MCO, mais toujours indispensables à la réactivité et à la souplesse d'emploi.

C'est le même esprit qui anime le programme Scorpion qui mettra en réseau *via* les radios *Contact* des vecteurs de haute technologie (*Griffon* et *Jaguar*) et des véhicules de gamme plus simple ou plus ancienne mais dont l'emploi sera optimisé par le partage de la situation tactique en temps réel.

En conclusion, l'avenir est à une différenciation des niveaux technologiques, non subie comme actuellement à cause de l'étalement des livraisons, mais assumée, anticipée doctrinalement et intégrée en réseau. En effet, comme évoqué plus haut, la spirale intégratrice de fonctions, permettant d'avoir moins de vecteurs, mais toujours plus chers à l'acquisition, l'emploi et à l'entretien, ne peut *in fine* que réduire les formats et renforcer les effets de la loi d'Augustine.

**Vers un nouveau modèle économique plus agile, plus pragmatique
et soutenant l'innovation de façon ciblée**

Hérité de la guerre froide, le modèle d'acquisition des équipements semble en partie dépassé dans les grands pays occidentaux et ne permet plus de contrôler efficacement le cycle, tant les raisons de surcoûts sont nombreuses et de champs différents. Les grandes puissances occidentales ont créé des outils pour évaluer ces processus. Aux États-Unis, le *Government Accountability Office*, comme le *National Audit Office* en Grande-Bretagne ou la Cour des comptes en France (et le Comité des prix de revient des fabrications d'armement français, CPRA) arrivent souvent aux mêmes conclusions de dérives des coûts et de changements de paramètres au sein des projets.

(25) Lettre hebdomadaire de la mission de Défense à Washington, n° 5, 2017.

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

Face à ce constat, des pistes émergent pour améliorer la rentabilité du système d'acquisition des équipements et donc maîtriser leur coût ⁽²⁶⁾. D'abord, adopter une approche plus commerciale. Ceci implique de lever certains freins, y compris idéologiques, au recours aux achats sur étagères, qui n'empêche pas l'achat auprès d'entreprises françaises ! Cette première piste pourrait être creusée en permettant comme le propose Emmanuel Levacher, président de Renault Trucks Defense, « *via* la loi, la mise à disposition à la Défense d'équipements récemment développés en vue de leur promotion à l'export » ⁽²⁷⁾.

Ensuite, il paraît utile d'adopter une démarche d'innovation incrémentale plutôt que de « prochaine génération » ⁽²⁸⁾. La maîtrise des coûts pourrait passer par la recherche de solutions techniques innovantes mais s'intégrant de façon incrémentale à des modèles existants, préparés très tôt, « nativement » à ces améliorations successives. Cette dynamique d'innovation créatrice est incitée aux États-Unis par le Pentagone avec la *DARPA*, doté de 3 Mds de dollars par an. Sous l'impulsion d'Ashton Carter, le secrétaire d'état à la Défense de l'Administration Obama, a été lancée la *Third Offset Strategy*, dotée de 20 Mds de dollars de 2017 à 2021 afin de compenser ce qui est vu comme l'érosion de la supériorité militaire américaine, notamment face aux technologies nivelantes ⁽²⁹⁾.

En se projetant plus loin, certains experts théorisent que la révolution robotique mettra fin à la loi d'Augustine en imposant de vraies ruptures technologiques dites disruptives ⁽³⁰⁾ freinant la course sans fin à l'amélioration de l'existant, processus qui, structurellement, engendre des surcoûts. Pour eux, « le champ de bataille de 2030-2040 comblera d'une manière absolument inédite munitions de haute précision, attaques cybernétiques, actions de guerre électronique, lasers et armes à hyperfréquences, avec un portefeuille de vecteurs combinant engins pilotés, robots, missiles cinétiques et électromagnétiques, opérations cybernétiques à distance » ⁽³¹⁾.

En France, avec des moyens financiers à notre mesure, il paraît essentiel à ce titre de conserver une capacité étatique de financement de R&D (recherche et développement) et de développement de programmes mais ciblée vers les domaines stratégiques notamment, tels que définis par le *Livre blanc* de 2008 ⁽³²⁾. Ceci dans un souci de préserver l'outil de la BITD nécessaire à notre indépendance, notamment autour de la dissuasion prise au sens le plus large. Cela implique d'accepter le risque d'abandonner des segments entiers qui peuvent être réalisés par d'autres. Cela a été accepté pour

(26) Renaud BELLAIS et Josselin DROFF, *Innovation, Technology, and Defence Procurement: Reform or Paradigmatic Shift?*, IGI Global, 2016, p. 205.

(27) Emmanuel Levacher, « L'armement terrestre, le combat de l'adaptation permanente », *RDN* n° 796, janvier 2017, p. 96-98.

(28) Renaud BELLAIS et Josselin DROFF, *op. cit.*

(29) Philippe GROS, « La Third Offset Strategy américaine », *Défense et industries* n° 7, juin 2016, p. 17-19 (www.frstrategie.org/publications/defense-et-industries/web/documents/2016/7.pdf).

(30) Renaud BELLAIS, « Technology and the Defense Industry: Real Threats, bad Habits, or New (Market) Opportunities? », *op. cit.*, p. 71.

(31) Christian MALIS, *Guerre et stratégie au XXI^e siècle*, Fayard, 2015, p. 213.

(32) *Livre blanc sur la Défense et la Sécurité nationale*, 2008 : « Les trois cercles de la politique industrielle » (sous-partie du Chap. 16, p. 264).

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

le fusil d'assaut et les armées françaises vont se doter entre 2017 et 2028 de 117 000 fusils *HK-416* produits par l'entreprise belge Heckler&Koch. Ceci peut également être fait en favorisant la R&D sur fond propre des entreprises et en intégrant des technologies civiles dans nos équipements, notamment les moins sophistiqués.

**Moderniser la conduite des programmes d'armement :
revoir les méthodes et les rôles des acteurs (instruction ministérielle 1516)**

La communauté de l'armement française a entamé récemment une démarche de modernisation des processus qui, à terme, devrait notamment avoir pour résultat de mieux maîtriser les coûts. Tout d'abord, la démarche de conception capacitaire a été modernisée par l'adoption récente de la Maîtrise d'architecture du système de défense (MASD). Cette démarche de cohérence rassemble tous les acteurs : Délégation générale pour l'armement (DGA) et son outil le Centre d'analyse technico-opérationnel de défense (CATOD), l'EMA, les armées et les industriels. La MASD cherche à aborder la réflexion capacitaire par système d'intérêt et non par simple remplacement du matériel précédent. Un système global d'appui feu numérisé sera par exemple recherché pour fusionner les systèmes *Atlas* (appui feu d'artillerie) et *Alliance* (appui feu air-sol) en cours d'obsolescence. De même, combiner les effets de radars au sol ou portés par des drones et/ou de capacités satellites permettra peut-être de succéder à l'*AWACS* dans certaines de ses fonctions. Cette remise à plat des périmètres capacitaires, partant du besoin militaire prévisible, semble vertueuse en ce qu'elle évitera des mises à jour intempestives de spécifications militaires car l'interopérabilité aura été anticipée au maximum, évitant des glissements de délais, donc de coûts. Pour autant, alors que son but est précisément d'optimiser les systèmes et donc les formats, cette approche MASD devra bien intégrer les besoins en nombre de vecteurs et de redondance, inhérents à la capacité de saturation et de contrôle durable du milieu présentés plus haut.

Cette démarche de cohérence capacitaire dans la conception des programmes, couplée à l'accélération du temps et aux capacités de la révolution digitale en cours entraîne une remise en question de la démarche très linéaire, longue et séquentielle induite par la directive 1516. Le programme *Frégates de taille intermédiaire (FTI)* a par exemple regroupé dans un même lieu, en plateforme, la DGA, l'EMA, la Marine nationale et les industriels concernés. Cette nouveauté a induit un fonctionnement plus proche de la spirale que de la ligne. Cela a permis, en intégrant de plus les exigences prévisibles des clients export futurs (équipage plus nombreux qu'une *Fremm*, tonnage plus réduit, technicité moins prégnante), de concevoir un navire de guerre plus rapidement, pour un coût moindre et exportable plus facilement. La rapidité de conception, de fabrication et de livraison est essentielle à la fois dans la satisfaction du besoin des forces et dans la maîtrise des coûts.

Vers une maîtrise des coûts de possession ?

Définir et intégrer la notion de coût de possession apparaît comme un graal difficilement atteignable tant les périmètres, les contrats et les contraintes d'emploi et de maintenance diffèrent. Pourtant, l'intégration des coûts de Maintien en condition opérationnelle (MCO) au plus tôt et de façon la plus précise possible dans les

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

programmes ⁽³³⁾ doit être un impératif d'autant plus fort que les armées, après l'acquisition réalisée sur le programme 146 (co-piloté CEMA-DGA) en récupèrent la charge sur le programme P178. Constaté qu'une heure de vol de *NH90* nécessite 40 heures d'entretien au sol (dont 18 heures de saisie informatique !) peut à cet égard poser question. Certes, le coût de MCO d'un matériel neuf est fort au début de sa mise en service et il est pris en compte dans le programme pour quelques années, mais sa maîtrise doit être un impératif dès la conception.

Savoir renoncer à une technologie ou émettre des spécifications raisonnables

Il peut parfois être nécessaire de ne pas choisir le niveau technologique maximal, notamment en termes de protection et en expliquer les raisons opérationnelles. S'il est compréhensible que les forces spéciales choisissent un véhicule faiblement protégé comme le *VTCFS* (*Véhicule tactique de combat pour les forces spéciales*), le choix pour les forces conventionnelles est moins simple et pourtant essentiel à l'efficacité opérationnelle qui requiert agilité, réactivité, furtivité et vitesse d'évolution sur le terrain face à un ennemi très volatil.

De plus, même si, on l'a vu, faire entrer dans la bulle numérique du combat de demain des véhicules moins performants est une piste à creuser, il faudra également savoir se limiter dans l'expression du besoin militaire numérique. L'exemple manqué de la numérisation de l'espace de bataille (attelage *SICF*, *SIR*, *SIT*, *SITEL*) des années 2000 a été à ce titre éloquent et doit servir de leçon pour une expression de besoin mesurée, modeste, rustique, conviviale et simple en vue des prochains systèmes. L'abandon en 2009 par l'armée américaine du *Future Combat System*, qui était destiné à remplacer le *M1 Abrams* et le *M2 Bradley* par un réseau de 18 plateformes connectées et interopérables est à ce titre un exemple de renoncement à un système tout technologique que même la puissance américaine a jugé inabordable ⁽³⁴⁾.

Promouvoir une innovation « frugale »

Un équipement militaire moderne doit évidemment, on l'a vu, répondre à des critères technologiques lui permettant de conserver ou de prendre l'ascendant sur l'ennemi. Mais il doit également être conçu dans un souci de simplicité d'emploi et de rusticité. Il est destiné à être employé dans des milieux hostiles voire extrêmes et prouvera sa valeur par sa fiabilité et sa robustesse comme par sa simplicité d'emploi par des opérateurs soumis au stress, à la fatigue et vulnérables à la saturation d'information. Cette simplicité de mise en œuvre et de maintenance est également un critère à l'export comme cela a été vu pour la *FTI*.

Les enjeux de l'innovation technologique devraient donc être la simplification, la baisse ou au moins la maîtrise des coûts tout en améliorant les performances. Cette démarche est adoptée dans toutes les branches de l'industrie pour laquelle la compétitivité

(33) Josselin DROFF, *Le facteur spatial en économie de la défense : application à l'organisation du Maintien en Condition Opérationnelle (MCO) des matériels de défense* (thèse) Économies et finances. Université de Bretagne occidentale, Brest, 2013.

(34) Scott O'NEIL, *op. cit.*

La loi d'Augustine est-elle une fatalité
pour les armées françaises à 10 ans ?

est directement liée au prix de vente du produit. L'exemple d'*Ariane 6*, développée actuellement par Airbus Safran Launcher, est à ce titre probant. L'objectif est clairement affiché, notamment pour faire face à la concurrence de SpaceX, de baisser de 40 à 50 % le coût unitaire du lancement tout en améliorant la performance du lanceur. Tous les efforts de l'innovation et de la R&D sont tendus vers cet objectif. De même, Thales met actuellement au point une jumelle de vision infra-rouge dont les capacités seront démultipliées par rapport aux générations précédentes pour un coût inférieur.

La situation de client unique, qui, on l'a vu devient de moins en moins vraie, ne doit pas empêcher le ministère de la Défense de profiter d'une telle dynamique vertueuse. C'est d'ailleurs ce qu'il fait *via* la DGA, avec des procédures comme *Rapid* ou *MIP* (*Mission pour l'innovation participative*) pour promouvoir les innovations concrètes, finançables et le plus souvent duales. Le système *Auxylium*, qui utilise la technologie du *smartphone* géolocalisé a été soutenu et financé dans ce cadre et équipe maintenant l'opération *Sentinelle*.

**

De ce fait, dans les années à venir et dans un contexte budgétaire qui ne s'améliorera pas, l'équipement militaire sera plus que jamais au cœur de trois forces dont la convergence est toujours un compromis, par nature, insatisfaisant : le besoin opérationnel, les exigences de la BITD et les capacités financières du pays.

Résister à l'effet d'entraînement, justifié sous bien des aspects on l'a vu, de la loi d'Augustine n'est donc pas une fatalité mais restera un enjeu existentiel pour les armées françaises dans les 10 ans à venir et au-delà. Les 3 armées ont besoin d'équipements dotés d'une technologie leur conférant une supériorité sur l'ennemi, mais également en nombre suffisant, fiables, rustiques et disponibles, c'est-à-dire d'un coût d'usage et de maintenance raisonnable.

Trouver cet équilibre tiendra à une modernisation de nos procédures programmatiques, visant notamment à les intégrer davantage et surtout à en raccourcir la durée ! Cela passera aussi par l'innovation, qui devra autant chercher à faire mieux qu'à faire moins cher et moins complexe. Enfin, garder un format correspondant aux menaces, sur un modèle complet, ambition réaffirmée de la France, sera avant tout l'objet de choix cruciaux du chef politique, conseillé par des militaires courageux, crédibles et éclairés.

La loi d'Augustine est-elle une fatalité pour les armées françaises à 10 ans ?

Éléments de bibliographie

- « Les lois d'Augustine », United Press International, 24 mai 1986.
- CREVELD (VAN) Martin, *The Age of Air Power*, PublicAffairs, 2011, 528 pages.
- DESPORTES Vincent, *La dernière bataille de France*, Gallimard, 2015, 208 pages.
- MALIS Christian, *Guerre et stratégie au XXI^e siècle*, Fayard, 2015, 352 pages.
- JOMINI Antoine Henri, *Précis de l'art de la guerre* (présentation de Bruno Colson), Perrin, 2001, 250 pages.
- CLAUSEWITZ (VON) Carl, *De la guerre* (présenté par Gérard Chaliand), Perrin, 2014, 448 pages.
- SCHWARZKOPF H. Norman, *Mémoires* (avec la collaboration de Peter Petre) Plon, 1992, 573 pages.
- ÉTAT-MAJOR DE L'ARMÉE DE TERRE, *Action terrestre future : demain se gagne aujourd'hui*, 2016, 69 pages (www.defense.gouv.fr/actualites/communaute-defense/action-terrestre-future-demain-se-gagne-aujourd-hui).
- SCALES Robert, *Scales on War: The Future of America's Military at Risk*, Naval Institute Press, 2016, 248 pages.
- FOUCAULT Martial, « Les budgets de défense en France, entre déni et déclin », *Focus stratégique* n° 36, avril 2012, 65 pages.
- ESQUERRE Hugues, *Quand les finances désarment la France*, Économica, 2015, 98 pages.

Les prestations de soutien commun du SCA à horizon 2020-2025 : évolutions comportementales des bénéficiaires et réponses à apporter

Anne TÊTE

| Commissaire en chef, auditeur de la 66^e session du CHEM.

Les armées françaises ont vu leur format, leur organisation, leurs équipements et leurs armements fortement évoluer au fil du temps et des conflits. Depuis plusieurs siècles, les intendances puis les commissariats de l'Armée de terre, de la Marine et de l'Armée de l'air, fusionnés en 2010 au sein du Service du commissariat des armées (SCA), les accompagnent dans la mise en œuvre d'un soutien quotidien qui s'adapte constamment aux besoins des forces, en temps de paix, de guerre, en métropole à l'étranger et sur les théâtres d'opération.

Au-delà d'une accélération ultrarapide des technologies, l'évolution de l'environnement géopolitique européen et mondial entraîne des changements profonds et inéluctables dont les conséquences pour les dix à quinze prochaines années restent encore difficiles à évaluer. Les projets « Cap 2020 », puis 2025, portés par le Chef d'état-major des armées (Céma), est destiné à adapter notre outil militaire de défense aux défis du XXI^e siècle. Décliné au sein des Armées directions et services (ADS), il va affecter non seulement leur cœur de métier mais également de manière significative le « soutien commun ». Pour accompagner ces évolutions sur différents axes, le service du commissariat des armées va porter un projet SCA 2017-2023.

En parallèle de ces mutations, arrivent sur le marché du travail, et donc dans les forces armées, plus gros recruteur de France, de nouvelles générations qui viennent bousculer celles qui les ont précédées. Nées à l'heure du digital, elles possèdent un « ADN modifié », et n'expriment plus les mêmes attentes, ni les mêmes priorités dans un monde incertain, dont elles ont compris qu'il n'aurait rien à voir avec celui de leurs parents.

Le soutien quotidien du militaire n'échappe pas à cette mutation. Il nous faut donc tenter de décrypter les attentes de ces nouvelles générations et envisager des pistes de solution à inventer pour moderniser le soutien, afin de ne pas rater le rendez-vous entre les armées et la jeunesse de France d'ici dix à quinze ans.

Un soutien évoluant dans le sillage de la transformation des armées et au gré de contingences externes

Le format des armées a été profondément transformé depuis la suspension du service national en 1995. Après les vagues annuelles de jeunes conscrits, les armées ont dû gérer la professionnalisation et développer une réelle attractivité pour donner envie à de jeunes Français de s'engager pour des contrats courts ou toute une carrière : charge aux armées de les former et de les fidéliser en leur proposant, entre autres, des conditions de vie rendant acceptables les sujétions imposées par la vie militaire, bref un soutien de qualité.

Après des années de niveau relativement faible d'intervention depuis la guerre d'Algérie, les forces armées françaises ont vu, à partir de la fin des années 1990, les opérations extérieures se succéder. Pour organiser leur vie quotidienne au sein des unités et sur les théâtres d'opération, chaque armée disposait en son sein de son propre service du commissariat, en charge de la définition et de l'acquisition des matériels et des services indispensables au fonctionnement quotidien et au soutien opérationnel. Ces moyens intégrés de soutien, intimement liés à leur armée de « tutelle » vivaient la relation de « soutenant-soutenu » dans un cadre hiérarchique, le soutien étant alors une émanation de l'autorité du chef du commandant de formation opérationnelle plutôt qu'un contrat de service ou de performance.

C'est dans le *Livre blanc sur la Défense et la Sécurité nationale* de 2008, et dans la réforme générale des politiques publiques que l'on trouve les origines des bouleversements en organisation, qui ont donné naissance au Service du commissariat des armées en janvier 2010. Service interarmées d'administration générale rattaché au Céma, le SCA s'est vu confier une partie des prérogatives assurées par les trois ex-commissariats d'armées. La création concomitante des bases de défense sur le territoire national et outre-mer et de leurs groupements de soutien, rattachés au SCA en septembre 2014, a finalisé l'organisation du soutien commun des armées, telle qu'on la connaît aujourd'hui. Ce mouvement a été accompagné de lourds efforts de rationalisation des moyens et de mutualisations, qui ont été très mal vécus par les armées.

Depuis 2010, le SCA, a été confronté à de multiples chantiers qui l'ont agité tant en interne ⁽¹⁾ que dans son cœur d'activité ⁽²⁾. Des crises lourdes ⁽³⁾ ont dû être gérées, tout en assurant au quotidien le soutien des militaires en opérations et sur le territoire national. En quelques années, c'est tout le paysage du soutien qui a été

(1) Création de la Direction centrale en 2010, du corps de Commissaires interarmées en 2013, renforcé par l'intégration d'officiers d'administration issus des armées directions et services entre 2014 et 2016, lourde déflation d'effectifs, nombreuses fermetures d'emprises et enfin rattachement hiérarchique des GSBdD en 2014.

(2) Diminution drastique des effectifs de soutien qui ne sont toujours pas terminées, rationalisation des systèmes d'informations qui s'est traduite par la suppression, l'évolution ou le développement de nombreux systèmes à marche forcée, identification des textes réglementaires à supprimer, créer ou faire évoluer, description des procédures à mettre en place, information et formation des acteurs de terrain et des armées etc.

(3) Mise en place de *Chorus* et adaptation de l'organisation des plates-formes achats finances en 2011, crise des *surstocks* de dossiers de frais de déplacement et de changement de résidence en 2011-2012, et bien entendu, reprise au niveau du SCA des fonctions de coordination et d'opérateur de la solde, domaine du ressort des armées jusqu'à la crise majeure de 2012.

transformé ⁽⁴⁾ contraignant les bénéficiaires des prestations à s'adapter à de nouveaux modes de délivrance, à des évolutions de procédures, de délais, de points de contacts etc., alors même que les prestations ne donnaient pas toujours satisfaction, et sans que les services de soutien ne bénéficient d'une mesure fine et sûre de la performance des différentes filières.

On l'aura compris, la problématique du soutien commun aux forces est devenue plus complexe à gérer, bouleversant les habitudes et impliquant de très nombreux acteurs, à la fois au sein du ministère (cabinet du ministre, ADS, directions centrales), mais aussi à l'extérieur avec Bercy, les comptables publiques pour la responsabilité financière confiée au SCA, et les sociétés extérieures, titulaires de contrats de prestations de soutien au profit des forces, sans oublier bien entendu, le militaire. Faisons davantage connaissance avec ces bénéficiaires des soutiens, tout aussi spécifiques que les prestations qui leur sont délivrées.

Une esquisse de profil des bénéficiaires des prestations

Aujourd'hui

« Bénéficiaires des prestations », cette périphrase au caractère un rien nébuleux recouvre pourtant une réalité, face à celui qui voudrait réduire le militaire à un simple « client », solution tentante et faussement simple. En effet, les militaires ne seront jamais des « clients classiques », n'ayant pas vocation à être de « simples consommateurs » de services et de prestations contre paiement. Un militaire est avant tout un opérationnel soumis à de fortes contraintes d'emploi, de disponibilité, de danger, ayant, dans le cadre de ses activités, des besoins spécifiques à satisfaire pour conduire les missions qui lui sont confiées. Un militaire sera à la fois et selon les prestations fournies, un usager (des lignes de cars), un administré (dans la solde), un client (au restaurant ou mess) ou encore un utilisateur (des flottes de véhicules) et surtout un soldat ⁽⁵⁾ quand il s'agira de l'habiller ou de lui fournir en opération et de façon professionnelle les services d'hygiène, de couchage, d'alimentation et de loisirs, bref de soutien de l'homme en opérations. Ces « clients qui n'en sont pas » sont déployés sur de multiples théâtres d'opération dans des environnements hostiles mais aussi dans de nombreuses emprises sur le territoire national, outre-mer et à l'étranger. Ce sont autant de situations qui font émerger des besoins spécifiques ⁽⁶⁾.

Enfin, le SCA soutient également du personnel civil, hors domaines opérationnels, qui sont autant de bénéficiaires comparables aux militaires en termes de besoins et d'exigences.

(4) Au-delà du soutien commun et de la création du SCA, c'est, au même moment, tout le paysage du soutien qui a été recomposé, donnant lieu à la création de directions interarmées spécialisées dites en « tuyaux d'orgues » dans le domaine informatique, de l'infrastructure, ou encore des munitions, le service de santé des armées ayant déjà été reconfiguré préalablement.

(5) Ou un marin, un aviateur.

(6) Le SCA assure le soutien de l'ensemble du ministère pour l'administration générale et le soutien commun, à l'exception du site de Balard, géré par la société Opale à travers un partenariat public-privé, et de certains volets du soutien assurés par le service parisien d'administration centrale, pour le personnel de son périmètre.

Le soutien du SCA bénéficie à plus de 200 000 militaires (plus les réservistes) et 60 000 civils ⁽⁷⁾ et donne la mesure du vivier de « clients » du SCA, qui doit s'adapter aux plusieurs milliers d'arrivées et de départs annuels, du militaire du rang à l'officier général. Multiples, les soutenus, peuvent se présenter à la fois en :

- **Individuel** et ce, dès leur premier jour de service au sein du ministère : militaire recruté sur la base d'un contrat ou d'un concours, réserviste opérationnel ou citoyen, bénévole ou collaborateur occasionnel, mais aussi militaire retraité ou encore sa famille.
- **Collectif** lorsque des unités, des groupes de personnes civiles et/ou militaires bénéficient de prestations communes et spécifiques liées à la mission qui leur a été confiée.

La qualité de service rendu émerge actuellement de façon imparfaite. Le « soutenu » dispose de différents canaux d'expression. L'armée, direction ou service d'appartenance sera son relais, puis le prescripteur auprès du SCA. Les instances de concertation récemment remodelées, CFM d'armées, CSFM, et maintenant APNM ⁽⁸⁾ sont autant de canaux ouvrant un accès direct et quasiment sans filtre aux plus hautes autorités. Par ailleurs, le militaire voire son conjoint, n'hésite plus à interpeller les médias, une autorité civile ou militaire, voire le ministre, pour faire remonter des dysfonctionnements qui pèsent sur son quotidien. On l'a vu dans lors de la crise de la solde.

Les équipes assurant le soutien de proximité s'expriment quant à elles à travers les relations régulières entretenues avec les responsables des « filières » de soutien, lors de visites d'autorités, à travers les indicateurs de gestion, dont on connaît les limites, ou encore grâce à des outils de sondage.

C'est donc à une multitude de besoins dans un paysage morcelé, que le SCA doit répondre en tout temps, tout lieu et toute circonstance, sans jamais perdre de vue la priorité opérationnelle.

Et demain

Sous réserve de la confirmation de choix politiques par le gouvernement nouvellement élu, l'idée d'un Service national universel ⁽⁹⁾ a été évoquée pour revitaliser la cohésion nationale et développer l'esprit et l'éducation civiques. La Garde nationale a vu le jour et va monter en puissance, composée en cible de plus de 80 000 réservistes. Des métiers vont particulièrement recruter notamment dans les domaines cyber ou renseignement. La part de militaires sous contrats personnalisés de durées variables devrait augmenter, de même que l'interarmisation ou, en phase avec la composition de la société, le nombre de soldats issus de la diversité. Les opérations extérieures, les échanges de personnels dans un cadre bi ou multilatéral avec les armées étrangères,

(7) DICO, *Les chiffres clés de la défense*, 2016.

(8) CFM : conseil de la fonction militaire, CSFM : conseil supérieur de la fonction militaire, APNM : associations professionnelles nationales de militaires.

(9) Service national universel à l'organisation duquel le ministère des Armées ne saurait absolument pas être le seul concourant.

les affectations dans des organisations internationales, ne devraient pas diminuer. Ces populations et lieux possibles d'affectation sont autant de paramètres à prendre en compte dans le portefeuille d'activités du soutien.

Les grandes tendances des générations Y et Z ⁽¹⁰⁾ et leur lien avec le monde du travail

Le chassé-croisé des baby-boomers et des générations dites Y et Z est un vrai sujet, notamment en France, où selon une analyse de l'OCDE ⁽¹¹⁾, le taux de crispation intergénérationnel est le plus fort. La moyenne d'âge des militaires est de 33,4 ans, inférieure de 14 ans à celle du personnel civil de la Défense ⁽¹²⁾. Environ 40 % des civils vont quitter le ministère d'ici sept ans entraînant un inévitable rajeunissement du personnel. Les armées recrutent chaque année plus de 15 000 jeunes, qui sont le reflet de la société française, elle-même en phase avec la « société mondiale » : alors que la moitié de la population mondiale a moins de 30 ans, celle-ci « s'uniformise », partageant les mêmes réseaux sociaux, les mêmes outils.

La première « génération numérique » a vu le jour, ce qui, aux yeux du philosophe Michel Serres, constitue « la troisième grande révolution anthropologique de l'histoire après l'invention de l'écriture et celle de l'imprimerie » ⁽¹³⁾. Comme toute révolution, celle-ci va tout bouleverser. Un monde est à réinventer, qui ne pourra plus être régi par les anciennes règles dépassées. Qui sera aux manettes de cette réinvention ? Les générations Y et Z, premières générations omniscientes, capables d'un clic ou d'un mouvement de doigt sur un *smartphone*, d'avoir accès au savoir, et de détenir un super-pouvoir, comme si elles avaient « externalisé leur cerveau dans la poche de leur jean » ⁽¹⁴⁾.

Le monde de la défense bénéficie d'une très bonne image auprès des jeunes, qui le considèrent comme particulièrement professionnel, réactif et efficace, le métier militaire étant bien perçu, jugé valorisant et motivant. Il attire un jeune sur dix ⁽¹⁵⁾. Mais parions que ce jeune motivé pourra être rapidement rebuté par les contraintes administratives, bureaucratiques et par ses conditions de vie quotidiennes, dès lors qu'il aura découvert l'autre face de la médaille du métier de militaire : les absences fréquentes de la maison, la délégation forcée de la vie quotidienne à la famille, les complexités de remboursement de frais, les aléas de l'habillement, les difficultés de connectivité à l'*Intradef* ou *Internet*, etc.

Les armées demandent des jeunes impliqués, capables de mettre en œuvre des équipements de plus en plus techniques. Les équipages resserrés des *Frégates multi-missions (Fremm)* de la Marine, dont les conditions de travail et de vie à bord sont très exigeantes, devront pouvoir trouver une contrepartie dans un accompagnement global

(10) La « génération Y » concerne les jeunes nés entre 1981 et 1999, la « génération Z » ceux nés après 2000.

(11) OCDE 2011, « Paying for the Past, Providing for the Future: Intergenerational Solidarity », 2011 (www.oecd.org/social/ministerial/session3payingforthepastprovidingforthefutureintergenerationalsolidarity.htm).

(12) DICOD, *Les chiffres clés de la Défense*, 2016 (www.defense.gouv.fr/actualites/articles/chiffres-cles-de-la-defense-2016).

(13) Michel SERRES, *Petite poucette*, Le pommier, 2012.

(14) Emmanuelle DUEZ, *The Boson Project*, (ré)engager les hommes (<http://thebosonproject.com/>).

(15) Enquête Dicod « Les jeunes et la défense » janvier 2016.

destiné à faciliter leur intégration mais aussi la vie de leur famille. Il en est de même pour le jeune militaire dans un Groupement tactique interarmes (GTIA) en opération extérieure, loin de chez lui pendant six mois, avant d'enchaîner sur d'autres périodes exigeantes.

Un regard nouveau sur le monde de l'entreprise (armées comprises) porté par les jeunes générations

Les jeunes générations cherchent à comprendre le « pourquoi »⁽¹⁶⁾, avant de s'intéresser au « comment », promeuvent l'exemplarité avant le statutaire. Elles sont portées par une ambition de s'accomplir avant celle de réussir. Pour ces raisons, elles sont davantage prêtes à avancer à côté des pas de leurs « pères » plutôt que dans les pas de ceux-ci. Aussi, devraient-elles être bien plus volatiles et flexibles, vis-à-vis de l'employeur, recherchant avant tout des expériences à forte valeur ajoutée et n'hésitant pas à enchaîner plusieurs postes pour poursuivre cette quête de sens. D'autant plus que de nombreux métiers qu'ils exerceront dans cinq ans n'existent pas encore aujourd'hui. Un tableau en annexe propose une sorte de portrait chinois, illustrant l'évolution des valeurs et des comportements professionnels des générations depuis les années 1950.

Les armées devraient pouvoir satisfaire ces jeunes générations dans leur quête de sens, notamment par le volet des activités opérationnelles, sous réserve que le soutien au quotidien ne soit pas le parent pauvre. Pourquoi les Google, Apple, Facebook et Amazon (GAFA) aiment-ils ainsi des bataillons de jeunes non seulement pour adopter leurs produits, mais aussi pour intégrer leurs rangs ? Le fait qu'ils se targuent de proposer une autre vision du monde, un « *massive transformational purpose* » semble entraîner l'adhésion des moins de 30 ans⁽¹⁷⁾. Ainsi, l'objectif recherché par ces jeunes générations, ne serait ni financier, ni basé sur l'atteinte des marqueurs matériels de la réussite. Ils montrent d'ailleurs un moindre attachement à la propriété, et ont intégré la précarité des carrières⁽¹⁸⁾.

Dans leur vie quotidienne et au travail, ils vont être à la recherche de l'immédiateté, ce qui les intéresse n'étant pas la recherche mais la réponse. Aussi devraient-ils rester perplexes face aux procédures administratives complexes et au carcan réglementaire parfois kafkaïen qui régit la plupart des domaines du soutien, alors qu'Amazon sait leur vendre en un frôlement d'écran tactile, et en livraison express, tout ce dont ils ont besoin dans leur vie personnelle. Chez le 15-24 ans, quasiment neuf internautes sur dix sont équipés de *smartphones*⁽¹⁹⁾, habitués au quotidien de Snapchat, WhatsApp, Facebook et autres Vine et Airbnb⁽²⁰⁾, le tout dans un environnement ludique où règne l'instantanéité dans les échanges et alors que les « serious games » envahissent le monde de l'entreprise, notamment sur les volets innovation et formation. Les armées ne

(16) « Y » pour « why ? », Olivier ROLLOT, *La génération Y*, PUF, 2012, 128 pages.

(17) Apple : « *Think different* », Amazon : « *Work hard, have fun, make history* » ou « Toujours au premier jour ».

(18) Thèse défendue par plusieurs consultants et analystes dont Julien Pouget.

(19) Étude Web observatoire de Médiamétrie du 3^e trimestre 2016.

(20) Ce sont toutes des applications gratuites : Snapchat permet de partager des photos ou des vidéos ; WhatsApp est un système de messagerie instantanée et d'appel ; Facebook est un réseau social ; Vine permet de créer des mini-vidéos de 6 secondes ; et Airbnb est une plateforme communautaire payante de location et réservation de logements de particuliers.

sauraient rester en dehors de l'accélération du numérique et de cette évolution vers le *gaming*.

Dans dix ans, 25 % de l'économie mondiale sera numérique. Mécaniquement et même s'il est difficile de le quantifier précisément, le contexte géopolitique sera profondément marqué par l'explosion de ces technologies qui pourraient modifier une grande partie des paradigmes existants. De même, le théâtre cyber, la maîtrise des réseaux et la gestion des données pourraient devenir très rapidement un enjeu sécuritaire critique pour les sociétés occidentales, mobilisant des ressources financières et humaines de plus en plus importantes. Le soutien des armées sera tout autant concerné.

Offre de « soutien commun des armées » : définition, carte actuelle et évolutions

Telle une société de « facilities management » ⁽²¹⁾ élargie et spécifique, « l'entreprise » SCA solde, indemnise déplacements professionnels et déménagements, nourrit, habille, transporte, livre, équipe en fournitures diverses, meuble, héberge, procure sur tous les théâtres des moyens sanitaires, de campement, d'hygiène et d'alimentation, gère des prestations de loisirs, assure l'entretien des espaces verts, etc. ⁽²²⁾. Son objectif ? Délivrer, conformément aux prescriptions des armées, des services de qualité, dans des délais compatibles avec le besoin opérationnel exprimé et au meilleur coût, avec des ressources humaines en propre limitées (98 % du personnel militaire servant au SCA est issu des armées), et dont le volume est en diminution constante.

Ce large périmètre exige autant de compétences et d'expertises, parfois très complexes, qui sont autant de métiers nécessitant des opérateurs professionnels et formés. Pour relever ces défis, le SCA après six années de montée en puissance a aujourd'hui organisé son modèle en filières de services, qui sont constituées d'organismes travaillant ensemble autour de chaînes de valeurs.

Ce schéma illustre l'enjeu du SCA d'offrir un service satisfaisant au plus grand nombre en ayant un volume d'activités de niveau « industriel ».



Service du commissariat des Armées, mars 2017

(21) Sociétés proposant des prestations de services, de maintenance et de gestion technique et administrative d'ensembles immobiliers tertiaires commerciaux industriels ou publics. Ces entreprises organisent et gèrent dans un modèle d'intégration de services et de performance sociale, les fonctions de soutien et de support aux entreprises (Source : syndicat professionnel des entreprises de multiservice immobilier).

(22) Au profit de personnel militaire et/ou civil.

Les pistes pour s'adapter à ces enjeux

Dans la plupart des régions du monde, nous utilisons l'électricité sans même y penser. Nous appuyons sur un interrupteur et trouvons normal que la lampe s'allume. Et plus nos besoins en électricité évoluent, plus nos exigences de qualité sont élevées. L'interrupteur est en quelque sorte le « *front office* », la partie utile et visible pour le client, qui ne regarde pas plus loin. Il ne se préoccupe pas du « *back-office* », une gigantesque infrastructure de barrages, de réseaux enterrés ou pas, de centrales nucléaires, etc. Il s'attend simplement à une « expérience client » supérieure toujours plus facile, plus rapide et plus complète, que ce soit en face-à-face, au téléphone ou *via Internet*. Dans le cas d'une entreprise privée, si le client n'obtient pas le service, il va chez un concurrent qui saura le lui fournir. Certes, le militaire n'a pas le choix de son fournisseur. Il est un « client captif » du service de soutien. Cela ne doit pas empêcher de lui proposer ce qu'il y a de meilleur par inspiration directe d'une « relation client » classique modernisée, sans laquelle on ne saurait attirer durablement les militaires des générations futures.

La révolution numérique du soutien

Les armées, au même titre que les institutions publiques, doivent imaginer les gains d'efficacité induits par les outils, les méthodes et les acteurs de cette révolution numérique, sinon elles seront débordées par de nouveaux entrants qui se seront investis à leur place, de cette mission de servir l'intérêt général. La révolution numérique impose la révision de plusieurs principes qui gouvernaient l'entreprise, les administrations, et aussi le monde militaire : l'intelligence du travail centralisée en peu de cerveaux, la recherche systématique de standardisation des produits et des processus, des travailleurs priés de se plier à ces règles centralisées et donc de devenir de simples exécutants sans réelle possibilité de faire émerger une initiative, le tout dans une logique généralisée du contrôle *a priori*, souvent tatillon et procédurier, en particulier dès qu'il s'agit de dépense publique.

Or, les nouvelles générations nous obligent à nous adapter à leur mode de fonctionnement où l'intelligence se déploie dans des réseaux ouverts, des communautés. Des citoyens engagés, des collectifs inventent très rapidement des solutions qui prennent une ampleur mondiale, nationale ou tout au moins adaptée à la communauté de Défense. En témoignent, les applications « sauvages » que l'on trouve d'un clic sur *Internet* : calculateurs de solde ou d'indemnités de remboursement de frais de déplacement, vente sauvage d'effets militaires de dotation, etc.

De la nécessité de développer une vraie démarche d'innovation pour les solutions numériques du soutien

Sous un *sponsoring* volontariste, engagé, doté de moyens financiers et humains, de petits groupes de travail de volontaires, futurs clients d'un produit numérique autour d'un indispensable développeur de code, pourraient en mode « agile » ⁽²³⁾,

(23) Les méthodes de développement « agiles » reposent sur un cycle de développement interactif, incrémental et interactif, et se veulent plus pragmatiques, impliquant au maximum le demandeur.

s'exprimer, tester, décider et créer une application ou un service, ainsi que le feraient des *start-up* d'État ⁽²⁴⁾. Il s'agit de passer d'une logique de corps d'armée ou d'escadre, à une logique de force spéciale souple et réactive. Il faudrait accepter que ce produit ne réponde pas à la panoplie complète des besoins préalablement identifiés, voire même que soient mis entre les mains des clients des produits non totalement aboutis. Il faudrait également accepter un droit à l'erreur. Mais cette démarche aura permis d'aller vite et de ne pas se laisser dépasser par des « créateurs sauvages » qui auraient comblé des lacunes sans qu'aucune garantie de service ne soit offerte. Il s'agit de ne pas être totalement décalé par rapport aux expériences similaires que chaque militaire vit sur son *smartphone* dans sa vie quotidienne privée pour ses besoins domestiques.

Une simple informatisation, c'est-à-dire une transposition des anciennes façons de faire dans des formulaires sur *Internet*, sans modifier les organisations, les services ni les relations entre ces organisations et leur client ne signifie pas être numérique et encore moins modernisé.

Reste à savoir où positionner les équipes innovantes. La lutte entre les « conservateurs » garants du fonctionnement de l'organisation et les « innovateurs » chargés de questionner ses rouages, si elle a lieu au même endroit, risque de conduire à des conflits. Mais n'est-ce pas Steve Jobs qui expliquait que « *If you don't cannibalize yourself, someone else will* » ? Les statuts de la fonction publique et des armées ne facilitent pas l'arrivée de compétences nouvelles qui ne sont pas transmises dans les écoles de formation initiales de la fonction publique. Or un besoin de profils plus variés, une volonté de libérer la capacité d'innovation et d'expérimentation, la tolérance face à l'erreur et la récompense du succès sont quelques-unes des clés de réussite de cette transformation numérique.

La puissance de comprendre et d'agir dont les collaborateurs bénéficient à leur domicile doit trouver un écho dans le monde professionnel, sinon naîtra une incompréhension, un décalage. La numérisation ne doit donc pas être appréhendée comme une seule automatisation ou un outil de réduction des effectifs. Il faut aller au-delà et confier aux gestionnaires professionnalisés d'une filière les fonctions complexes à forte valeur ajoutée qui ne peuvent être traitées dans le flux, et leur faire instruire les volets humains qui se cachent derrière les dossiers.

Du Big Data aux objets connectés

Qui au sein des armées comme dans sa vie privée, n'a pas rêvé d'être traité comme un individu autour duquel s'organisent l'ensemble des acteurs concernés par son problème ? Qui n'a pas rêvé de voir une institution régler complètement son problème au lieu de se retrancher dans son périmètre « contractuel » ?

Pour répondre à cette attente, le ministère aura à affronter le cap du fameux *Big Data*, c'est-à-dire la valorisation et l'exploitation de la somme incroyable d'informations

(24) Pierre PEZZIARDI et Henri VERDIER, *Les startups d'État à l'État plateforme*, Fondation pour l'innovation politique, janvier 2017, 56 pages (www.fondapol.org/etude/pierre-pezziardi-et-henri-verdier-des-startups-detat-a-letat-plateforme/).

dont il peut disposer utilement à partir des données issues des innombrables systèmes d'information. Opération lourde et complexe s'il en est, coûteuse et sensible d'un point de vue protection des données, l'utilisation du *Big Data* n'aurait pas comme dans les entreprises privées des enjeux commerciaux ou de *marketing*, mais bien d'efficacité et de personnalisation du soutien.

- C'est, par exemple, tout le rituel d'instruction des dossiers personnels qui pourrait être modifié, simplifié et partagé, selon le principe du « dites-le nous une fois ». Un militaire déclarant la naissance d'un enfant doit aujourd'hui fournir un justificatif à plusieurs services internes au ministère, mais aussi auprès d'autres administrations (allocations familiales, impôts, etc.). Il faudra bien un jour envisager de ne lui demander au titre de l'Administration qu'une seule et unique fois sa pièce justificative, pour ensuite au sein des armées, voire de façon plus large, adapter les offres de service et de soutien à sa nouvelle situation. Un coffre-fort électronique individuel sécurisé devra être accessible à chaque militaire lui permettant de retrouver à tout moment et depuis n'importe quel point d'accès *Internet* la totalité des pièces constitutives de sa situation administrative ⁽²⁵⁾.

Dans l'esprit du simulateur *Internet* « mes aides.gouv.fr », ou encore « mon service public.fr », des sites équivalents destinés à la communauté militaire permettraient de regrouper des informations aujourd'hui dispersées sur de nombreuses pages gérées par autant d'organismes différents, ne procurant au militaire en recherche d'information que découragement et sentiment d'impuissance. Il passe aujourd'hui à côté de nombreuses offres et informations par incapacité à les dénicher dans le foisonnement des pages *Intradef*, si tant est qu'il dispose d'un accès, ce qui est peu le cas dans l'Armée de terre par exemple.

Demain, lorsqu'un militaire déménagera, c'est, à travers un point de contact unique, tout une offre d'accompagnement de sa famille qui devrait pouvoir lui être proposée, allant jusqu'à l'aide pour trouver un logement ou la rentrée scolaire des enfants, ainsi que des conditions administratives et d'organisation du déménagement simplifiées.

- Une autre piste consisterait à transformer le GSBdD (Groupement de soutien de la base de Défense) en guichet unique d'intégrateur du soutien. Accessible par plusieurs canaux, ce guichet unique, tel une conciergerie d'entreprise sophistiquée, pourrait prendre les rendez-vous vers le centre médical des armées, recevoir des demandes d'intervention informatique ou de maintenance dans les locaux ou encore offrir des services de *pressing*, révision de voitures, etc.

Les technologies qui simplifient et sécurisent la vie des entreprises privées, vont continuer à évoluer et leurs applications doivent être étudiées dans le domaine du soutien. Les puces *RFID* ⁽²⁶⁾, les différentes applications des imprimantes 3D, les

(25) Le projet *Ensap* (*Espace numérique sécurisé de l'agent public*) est une piste intéressante si elle est conduite à terme.

(26) « *Radio frequency identification* », permet de mémoriser et de récupérer des données à distance en utilisant des « marqueurs » appelés radio étiquettes, petits objets tels des étiquettes qui peuvent être collés sur ou incorporés dans des objets. Contenant une antenne associée à une puce électronique, ils peuvent recevoir et répondre aux requêtes radio émises depuis l'émetteur récepteur.

QR codes ⁽²⁷⁾, les objets connectés doivent entrer dans la vie quotidienne des militaires, autrement qu'à travers leurs équipements opérationnels sophistiqués, qui eux bénéficient déjà de ces avancées. Des réflexions sont en cours. Le temps est notre ennemi. Produisons rapidement des *proof of concept*, afin de déterminer si des prototypes sortis de la réflexion innovante de petites équipes, sont rapidement utilisables, ou s'il faut d'abord prévoir des évolutions métiers (processus ou réglementation), ou encore pour s'assurer que la définition du service que l'on souhaite proposer est bien définie et partagée ⁽²⁸⁾.

Les prévisions de la Foresight Factory ⁽²⁹⁾ pour 2025 mettent en avant la prégnance de l'intelligence artificielle qui permettra d'améliorer les services en temps réel sur différentes plateformes, la prépondérance des communications visuelles sur les médias sociaux et le fait qu'environ 50 % des consommateurs posséderont un ou plusieurs objets connectés, capables de collecter de nouvelles données de type comportementales.

Ainsi, doté de nouveaux outils numériques et de *process* de travail totalement renouvelés, l'opérateur de soutien ne serait plus seulement un pourvoyeur de solutions mais rendrait aux soutenus du temps de travail, qui pourrait être consacré aux activités du cœur de métier du soldat.

Une condition de la réussite : partager une formidable ambition

Et si le ministère des Armées dans son ensemble partageait une « ambition démesurée », de celle que préconisent les auteurs du livre *Massive Transformation Ourpose* ? Déclinée au domaine du soutien, il s'agirait de transformer l'environnement de travail, à la fois en adaptant les idées des autres, mais aussi en développant des innovations propres à satisfaire les besoins des soutenus. Cette ambition, si elle est partagée pourra créer les conditions du succès. Si des barrières financières, techniques, ou réglementaires doivent venir brider les initiatives, alors ce temps consacré à être ambitieux sera du temps perdu et le militaire devra se contenter de petites améliorations sans envergure et vite dépassées.

Les acteurs de cette ambition sont l'État-major des armées, en tant que donneur d'ordre et les armées en prescripteurs professionnalisés de besoin. Charge ensuite à l'opérateur SCA de proposer des offres de service, non en termes de moyens, mais d'effets à obtenir, et de monter le dispositif *ad hoc* ⁽³⁰⁾.

Cette ambition ne saurait se passer :

- D'une réflexion portant sur l'externalisation de certains services. Par exemple, les prochaines diminutions d'effectifs prévues au Commissariat des armées notamment

(27) Type de code-barres en deux dimensions, constitué de modules noirs sur fond blanc. L'agencement de ces points définit l'information que contient le code.

(28) Par exemple, le concept « d'agence de voyage » au sein du ministère de la Défense.

(29) Foresight Factory (précédemment « the Future foundation »), Entreprise internationale basée à Londres, qui analyse les tendances des marchés pour identifier les ruptures et permettre aux entreprises commerciales d'anticiper les besoins et attentes de leurs clients.

(30) Un peu sur le modèle de l'Armée de terre qui a obtenu de la Préfecture de police de Paris de mettre à disposition des troupes *Sentinelles* sur des effets à obtenir et non sur des demandes d'effectifs.

dans le domaine de la restauration militent en sa faveur. Diminutions qui ne devront pas faire perdre de vue les contraintes opérationnelles (continuité du service public en situation d'urgence) ou encore des efforts d'amélioration de la qualité des prestations sur des emprises emblématiques.

• D'une démarche volontariste d'évolution ou de simplification réglementaire. Le domaine des droits financiers individuels notamment ne peut raisonnablement rester en l'état. Deux pistes de réflexion concernant les déménagements pourraient être envisagées, avec à la clé une solution à prévoir dans la durée :

- déterminer des forfaits de bon niveau tant en montant financier qu'en qualité des prestations, en fonction des destinations, comme cela peut se faire dans d'autres ministères ;
- ou encore mettre en place un marché national proposant des solutions de bon niveau, modernes et adaptées, évitant aux administrés d'entrer dans les difficiles négociations avec les déménageurs dans le cadre de contrats de droit privé ;
- ou encore envisager comme cela peut se faire dans d'autres pays tel que le Canada, le remboursement des frais d'agence immobilière, de frais de notaire et de certaines taxes dès lors que le militaire doit quitter un logement dont il est propriétaire.

La solde est également un domaine très réglementé, d'une rare complexité, où les indemnités se cumulent (ou pas) aux primes, dans un labyrinthe de textes et de lourdes contraintes informatiques. Ces dernières peuvent être aggravées par ricochet, à l'occasion de projets gouvernementaux, tels que le prélèvement à la source ou la simplification du bulletin de paye. La rémunération du personnel militaire, très fortement touchée par la crise *Louvois*⁽³¹⁾ de 2012, ne pourra pas durablement résister à une révision de la politique salariale. Outre une meilleure lisibilité, et une juste reconnaissance des engagements et des sujétions des militaires, cette nouvelle architecture pourrait faciliter l'intégration de la solde dans des systèmes d'information gérables et ainsi libérer les ressources importantes qui y sont actuellement consacrées.

**

Nous vivons une accélération incroyable de notre environnement, mouvement tout à la fois porteur de promesses et inquiétant.

Sans forte volonté politique, réflexion et démarches en profondeur pour faire émerger les nouveaux métiers, intégrer les nouvelles technologies, renouveler les relations humaines spécifiques entre soutenus et soutenant, et pour proposer des solutions innovantes, le ministère pourrait passer à côté de la modernisation. Il risquerait de marcher à deux vitesses, avec trois armées fortement montées en gamme technologiquement sur le volet opérationnel et un soutien repoussoir et daté, qui freinerait la

(31) Projet lancé en 1996, le *Logiciel unique à vocation interarmées de la solde (Louvois)* est progressivement entré en service en 2011 mais certains militaires ont été trop payés, d'autres moins, voire pas du tout. Les nombreuses erreurs de calcul étaient liées principalement à la grande diversité des primes. Le logiciel sera remplacé par *Source Solde* d'ici 2019.

dynamique d'ensemble des armées. Le ministère est déjà passé à côté de certains projets pourtant prometteurs : la carte *CIMS* ⁽³²⁾, multiservices en théorie, ne permet pas, à l'exception de Balard, de payer son repas dans les cercles, ni même de franchir un portillon automatisé sur tous les sites du ministère.

La numérisation du soutien n'est que la partie émergée de l'iceberg. Loin sous la surface se révèlent les freins à lever pour moderniser le soutien.

Ces freins sont à la fois :

- **Techniques** : Les politiques informatiques interarmées et de sécurité des systèmes d'information sont très prégnantes à juste titre alors que la menace cyber est intense. Toutefois, ces menaces et risques ne doivent pas, par précaution, conduire à l'immobilisme. *Intradef* n'est pas l'écrin idéal de la modernisation du soutien. Les bénéficiaires attendent de pouvoir utiliser leur *smartphone* et donc d'utiliser le réseau Internet. Les transactions financières des grands groupes bancaires se font de façon sécurisée sur *Internet*. Les données des soutenus doivent pouvoir être cryptées ou rendues anonymes, le traitement de nos populations sensibles ⁽³³⁾ devant certes être organisé à part. Opter, concernant le développement du numérique, pour l'équipement de toutes les armées françaises de téléphones portables sécurisés ou, préférer utiliser une technologie *Internet* à durcir est un pas majeur et qui doit être accompagné des financements dédiés, mais indispensable et rapide si on veut avancer.

- **Organisationnels** : Depuis la création du SCA, les armées n'ont de cesse, chacune à leur façon, de tenter de reprendre une part plus ou moins grande de ce qu'elles estiment nécessaire à leur soutien « consubstantiel ». De son côté le SCA, au terme de six années tendues jalonnées de crises, de chantiers majeurs et de contraintes multiples est progressivement monté en gamme et rend le service, bien que des marges de progression soient encore clairement identifiées. La « ré-internalisation » partielle de certains secteurs au sein des forces armées est une tentation, au risque de voir s'effondrer la dynamique collective que le SCA s'efforce de construire aux côtés des armées, et peut être au détriment des bénéficiaires du soutien qui verraient les repères de leur environnement quotidien une nouvelle fois bouleversés.

De gros chantiers s'ouvrent concernant la défense et les équipes de toutes les couleurs d'uniforme ainsi que les civils, qui ont énormément donné ces dernières années, attendant que leurs chefs avancent de concert et non en ordre dispersé, prémices de l'échec. Les jeunes générations de militaires sous les drapeaux en 2020-2025 ne comprendraient pas que leur intérêt commun soit passé en second plan.

Dans ce monde en mouvement perpétuel et accéléré, où l'agile mangera l'inerte, et « ce qui ne bouge pas à la vitesse du monde est condamné à périr » ⁽³⁴⁾, un front uni

(32) *Carte d'identité multiservices.*

(33) Au sens de la LOPPSI II (Loi d'orientation et de programmation pour la performance de la sécurité intérieure) et de l'arrêté du 9 mai 2011.

(34) Hartmut ROSA, *Aliénation et accélération, vers une théorie critique de la modernité tardive*, La Découverte, 2013, 154 pages.

de la défense sera plus fort face aux oukases de l'interministériel et au rythme d'évolution des technologies. La modernisation numérique est un enjeu de compétitivité et de souveraineté. Le tempo de modernisation du soutien est actuellement trop lent par rapport aux acteurs civils du métier. Le *statu quo* ouvrira la porte à des acteurs innovants extérieurs, sans garantir la maîtrise des informations. Le ministère ne pourra agir seul dans cette modernisation du soutien. Il devra également composer avec les organes interministériels ⁽³⁵⁾ travaillant sur le projet de l'État numérique, et s'adjoindre les compétences spécifiques qui lui font aujourd'hui défaut.

Les jeunes sont prêts à s'engager pour la défense de leur pays, ils l'ont montré ces derniers mois. Au ministère des Armées de leur ouvrir les portes, de se tourner vers les écoles d'ingénieurs, de développement informatique et de commerce, pour les associer aux travaux d'innovation par le biais d'engagement à servir dans la réserve ou dans la réserve citoyenne. Il s'agit de les associer à la réalisation d'une ambition commune et partagée : la modernisation du soutien commun des armées.

Éléments de bibliographie

BARET Laëtitia : « À quoi ressemblera la relation client en 2025 ? », *E-Deal*, 3 novembre 2011 (www.e-deal.com/pige-vous/quoi-ressemblera-la-relation-client-en-2025/?lang=fr).

FORESIGHT FACTORY, site officiel (www.foresightfactory.co).

GRANGE Benjamin, *Le dirigeant et l'accélération*, Débats publics, 2015, 103 pages.

HARTMUT Rosa, *Aliénation et accélération. Vers une théorie critique de la modernité tardive*, La Découverte, 2013, 154 pages.

HEWLETT-PACKARD, *Le Livre blanc pour les décideurs : Les clients influencent-ils vos décisions en matière de technologies ? Peut-être le devraient-ils ?*, 2014, 8 pages.

NEMRI Mehdi, *Demain l'Internet des objets*, France stratégie, 2015 (www.strategie.gouv.fr/publications/demain-linternet-objets).

PEZZIARDI Pierre et VERDIER Henri, *Des startups d'État à l'État plateforme*, Fondation pour l'innovation politique, 2017, 56 pages (www.fondapol.org/etude/pierre-pezziardi-et-henri-verdier-des-startups-detat-a-letat-plateforme/).

POLÈRE Cédrix, « Modernisation de l'action publique : l'expérience usager au cœur de la relation avec l'administration – Interview de M^{me} Laure Bonneval (chef de projet SGMAP) », *Millénaire 3*, La prospective de la métropole de Lyon, 12 décembre 2014 (www.millenaire3.com/).

POUGET Julien, *Intégrer et manager la génération Y*, Vuibert, 2010, 208 pages.

ROLLOT Olivier, *La génération Y*, PUF, 2012, 128 pages.

SERRES Michel, *Petite poucette*, Le pommier, 2012, 84 pages.

(35) SGMAP : Secrétariat général pour la modernisation de l'action publique et DINSIC : direction interministérielle du numérique et du système d'information de l'État.

Les prestations de soutien commun du SCA à horizon 2020-2025 :
évolutions comportementales des bénéficiaires et réponses à apporter

ANNEXE : PORTRAIT CHINOIS DES DIFFÉRENTES GÉNÉRATIONS EN ENTREPRISE

Source Managériis, analyse réalisée par les équipes de Dentsu consulting. Cité dans Benjamin GRANGE, *Le dirigeant et l'accélération numérique*, Débats publics, 2015.

	La génération de la guerre (nés avant 1950)	La génération 60 (nés entre 1950 et 1970)	La génération de la crise (nés entre 1970 et 1985)	La génération Y (nés entre 1985 et 1995)	La génération Z ou alpha (nés à partir de 1996)
Événement structurant	<ul style="list-style-type: none"> - Seconde Guerre mondiale. 	<ul style="list-style-type: none"> - Guerre du Vietnam, contestation des années 1960. 	<ul style="list-style-type: none"> - Crise économique, Sida... 	<ul style="list-style-type: none"> - Chute du mur de Berlin, début d'Internet, généralisation de la téléphonie mobile. 	<ul style="list-style-type: none"> - Attentats du 11 septembre 2001, état récurrent de crises économiques, génération tablette.
Valeurs fondamentales	<ul style="list-style-type: none"> - Loyauté, ordre, travail. 	<ul style="list-style-type: none"> - Optimisme, épanouissement par la réussite professionnelle et personnelle, recherche d'un idéal 	<ul style="list-style-type: none"> - Scepticisme, « compte sur toi-même », profite de la vie aujourd'hui. 	<ul style="list-style-type: none"> - Impatiente « dans l'instant », autoentrepreneur, ouverte sur le monde, en recherche de sens et d'éthique. 	<ul style="list-style-type: none"> - Rapport décomplexé à l'erreur, assume le fait de « ne pas savoir ».
Attitude vis-à-vis de la hiérarchie en place	<ul style="list-style-type: none"> - « Un supérieur se respecte en toutes circonstances ». 	<ul style="list-style-type: none"> - « L'opinion de mon supérieur conditionne ma réussite future, je dois donc le satisfaire ». 	<ul style="list-style-type: none"> - « Un supérieur n'est légitime que lorsqu'il mérite sa place ». 	<ul style="list-style-type: none"> - « <i>Le manager</i> doit davantage aider et donner du sens au travail plutôt que contrôler ». 	<ul style="list-style-type: none"> - Ne veut pas être canalisé, ni marqué à la culotte, contact direct.
Feedback favori en situation de projet	<ul style="list-style-type: none"> - Le moins possible et seulement quand il faut recadrer. 	<ul style="list-style-type: none"> - À intervalles réguliers de façon formelle. 	<ul style="list-style-type: none"> - Régulièrement de façon formelle et informelle, et en permettant au collaborateur de dire aussi ce qu'il pense des autres. 	<ul style="list-style-type: none"> - En permanence de façon informelle en permettant au collaborateur de dire aussi ce qu'il pense des autres et de ses supérieurs, S attend à être coaché au quotidien. 	<ul style="list-style-type: none"> - Au fil de l'eau, besoin constant d'être rassuré, encouragé sans être asphyxié.
Attitude vis-à-vis des technologies de l'information	<ul style="list-style-type: none"> - Déné initial et souvent passionnel, ralliement par raison, une fois la praticité démontrée. 	<ul style="list-style-type: none"> - Nécessité de s'adapter à un rythme croissant d'innovation technologique, différents degrés d'acceptation des TIC. 	<ul style="list-style-type: none"> - Pratique de l'informa-tique personnelle des jeux vidéo puis d'Internet, usage hétérogène des réseaux sociaux. 	<ul style="list-style-type: none"> - « <i>Always on</i> », Dépendance aux médias technologiques mobiles MP3, SMS, réseaux sociaux, consoles de jeux. 	<ul style="list-style-type: none"> - Leur donner des défis digitaux, des missions ponctuelles assorties d'objectifs et les laisser travailler par eux-mêmes.

Associations professionnelles nationales de militaires et dialogue social dans les forces armées

Frédéric BOUDIER

| Colonel (gendarmerie), auditeur de la 66^e session du CEM.

Par deux arrêts du 2 octobre 2014, la Cour européenne des droits de l'homme (CEDH) a condamné la France pour non-respect de l'article 11 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales pour l'interdiction faite aux militaires de créer des groupements professionnels à caractère syndical dans les armées. Tirant les conséquences de cette jurisprudence européenne, la France a mis en conformité sa législation. La modification de cette interdiction générale et absolue aux militaires en activité de service de créer et d'adhérer à des groupements et associations à caractère politique ou syndical garantit concomitamment à ces organismes la reconnaissance d'un droit au dialogue social avec la hiérarchie militaire au sein du Conseil supérieur de la fonction militaire (CSFM). Ce changement de paradigme suscite questions et inquiétudes au sein de la communauté militaire qui voit dans cette évolution un coin potentiellement enfoncé dans ce qui constitue la force traditionnelle des armées, à savoir l'obéissance au chef.

De ce point de vue, il est tout d'abord loisible de s'interroger sur le bien-fondé de la concertation au sein d'une institution qui, au nom d'une efficacité salubre, ne peut souffrir la moindre forme de cogestion. Il convient ensuite de se pencher sur la genèse et le nouveau visage du dispositif rénové de dialogue social mis en place par la Loi. Enfin, certaines perspectives d'évolutions potentielles ou souhaitables pourront être évoquées concernant une nouvelle architecture qui n'en est qu'à ses balbutiements.

Le bien-fondé de la concertation

De saines instances de concertation rendues nécessaires

Avant d'envisager les formes que doit prendre la concertation dans la communauté militaire, cette dernière doit s'entendre sur la définition même de la concertation et surtout sur sa finalité, ce qui est loin d'être totalement partagé.

Un courant, sans doute minoritaire au sein des armées, continue en effet de penser que la concertation, d'une part, contredit le principe même de l'autorité militaire en induisant la cogestion et, d'autre part, s'avère inutile puisqu'il appartient au chef militaire, à tous les échelons, de veiller aux intérêts de ses subordonnés selon les

dispositions du code de la Défense. À ce titre, de telles instances seraient au mieux superflues et au pire dangereuses pour la discipline dans les armées et la réalisation des missions.

Ce point de vue appelle quelques éléments de réponse. Pour éviter le risque de tomber de fait dans une cogestion qui fragilise, au moins en France, l'action de certaines institutions civiles, il convient en premier lieu de distinguer ce qui relève de la concertation et ce qui doit rester l'apanage du chef militaire :

- Au stade de la réflexion et de la programmation la concertation avec les échelons subordonnés ne peut qu'enrichir les analyses et garantir la prise en compte des préoccupations et de tous les paramètres en jeu. Elle ne devrait sans doute pas être décorrélée de l'exercice du commandement puisqu'elle lui est consubstantielle. Elle aide en effet le décideur à exercer un commandement éclairé, enrichi de l'expérience, des contraintes et du ressenti de ses subordonnés.
- Une fois la décision prise, tenant compte des observations formulées par les subordonnés ou leurs représentants, vient le stade de l'exécution ou de la mise en œuvre au cours de laquelle la concertation s'efface naturellement. Une concertation bien menée aide par ailleurs à susciter l'adhésion et annihile la contestation, ce qui s'avérera profitable à la bonne exécution de la mission.

Dès lors que ces différentes phases sont bien appréhendées par tous les acteurs concernés, la concertation correctement encadrée n'a pas de raison de dériver vers la cogestion. Il ne s'agit en effet pas de décider conjointement mais juste d'éclairer le chef pour ce qui sera sa seule décision.

À ceux qui continuent par ailleurs de penser qu'il appartient au seul chef de veiller aux intérêts de ses subordonnés, il est aisé de répondre en premier lieu que pour que ce même chef dispose de vrais relais parmi eux, surtout dans les grandes unités, relais que sont justement les militaires investis d'un mandat de représentation ou de concertation. Il convient par ailleurs de remarquer que dans la société française actuelle, le chef militaire, quel que soit son rang, a en fait besoin de s'appuyer sur les instances de concertation pour être mieux entendu à l'extérieur et permettre à la condition militaire de ne pas décrocher des évolutions de la société en général, et de la fonction publique civile en particulier. Pour illustrer ce propos, et pour ne citer qu'un exemple, il n'est pas anodin de rappeler que la transposition aux militaires de mesures relatives aux bas salaires accordées aux fonctionnaires civils n'a été obtenue ces dernières années, après d'âpres et longues discussions interministérielles menées par l'autorité militaire, qu'à la veille de la clôture de sessions du CSFM par le ministre. Il est vraisemblable que sans la pression des instances de concertation, les arbitrages interministériels sur des questions qui ne visaient pourtant qu'à garantir une simple équité de traitement entre civils et militaires auraient été défavorables aux militaires ou sans cesse reportées. Ce constat peut être déploré mais il ne peut être que difficilement contesté.

Au sein d'une société qui agit ou réglemente en fonction des rapports de force, le réalisme conduit à considérer que les instances de concertation sont le meilleur appui au commandement pour défendre justement la condition militaire. En effet, l'idée

selon laquelle elles véhiculent directement, sans le filtre de la hiérarchie, les aspirations des militaires de tous grades, leur confère un poids particulier et inégalé qui tient aux caractéristiques même du dialogue social à la française.

Des instances qui doivent être renforcées et valorisées

Il est regrettable de constater que les grandes étapes qui ont rénové ou renforcé la concertation dans les armées ont fait suite à des crises : la création du CSFM intervient en 1969 au lendemain d'une crise sociétale où l'autorité était remise en cause. La création des CFM d'armée intervient en 1990, juste après la contestation née dans les rangs de la gendarmerie à travers les lettres anonymes, moyen déplorable d'expression de problèmes réels mais aussi... seul procédé d'expression publique des militaires de l'époque à s'être avéré efficace. Pour ce qui concerne la gendarmerie, cette dernière a renforcé ses instances de concertation locale en instaurant des présidents de catégorie après une nouvelle crise dénonçant le manque chronique de moyens et la multiplication des missions en 2001. Chacune de ces crises avait en fait démontré :

- que les outils de concertation de l'époque étaient inefficaces pour évaluer et apaiser des tensions et difficultés réelles ;
- que les quelques prises de position courageuses de certains chefs pour relayer le mal-être de leurs subordonnés étaient restées lettres mortes.

Forte de ces expériences malheureuses, la gendarmerie a, au début des années 2000, résolument décidé d'être proactive plutôt que réactive en renforçant ses instances de concertation, non pas sous la pression d'une nouvelle crise qu'elle ne pouvait se permettre, mais de manière réfléchie et partagée. Ainsi, l'élection de représentants des militaires a été généralisée à chaque échelon de commandement infranational à partir de l'échelon compagnie. Force est de constater que, depuis le renforcement des instances de concertation et malgré une pression opérationnelle croissante dans des périodes de manques de moyens, ces instances ont pleinement joué leur rôle, non pas contre mais aux côtés de la hiérarchie, éclairant leur chef sur les difficultés matérielles et humaines rencontrées tout en accompagnant auprès de leurs camarades les orientations du commandement.

Ce modèle intégré, qui mérite sans cesse d'être adapté et amélioré, nécessite cependant une action proactive de la hiérarchie car la crédibilité du représentant d'une unité repose sur sa légitimité qu'il tire idéalement de son élection et sur la formation octroyée en début de mandat afin de l'aider à mieux cerner sa fonction. Un militaire issu d'une unité opérationnelle appelé à exercer un mandat national a en effet besoin d'appréhender l'environnement interministériel dans lequel son institution évolue et les contraintes qui s'y rapportent s'il veut comprendre les enjeux et rendre des avis éclairés. Un militaire exerçant un mandat local doit, quant à lui, être sensibilisé aux techniques d'écoute, à la résolution de conflits interpersonnels ou au travail en réseau avec d'autres acteurs ayant à connaître des problèmes humains (médecin, psychologue, assistant social...) au sein de l'institution.

Si les instances de concertation nationales sont identiques entre forces armées, les instances locales ont été développées en fonction des besoins et de la culture de chacune des grandes entités composant la communauté militaire.

Du fait de son insertion au ministère de l'Intérieur et de son contact permanent avec le monde civil, mais aussi en raison de la dispersion de ses unités sur le territoire national, la Gendarmerie nationale a développé au cours des vingt dernières années le réseau le plus dense de représentants des personnels militaires. Elle a par ailleurs densifié l'action de son CFMG en instaurant en son sein par élection un groupe de liaison qui rencontre régulièrement les plus hautes autorités de l'État (président de la République, ministre de l'Intérieur et garde des Sceaux, Défenseur des droits...).

L'émergence d'un nouveau modèle de concertation

Genèse des APNM

En réponse à la condamnation de la France par la Cour européenne des droits de l'homme (CEDH) pour avoir interdit à ses militaires le droit d'association à caractère professionnel en vertu de son statut général des militaires, la loi n° 2015-917 du 28 juillet 2015 a modifié en profondeur l'exercice de la concertation dans les armées.

Tout d'abord, la loi définit clairement ce qui ressortit de la condition militaire ⁽¹⁾ en modifiant l'article L. 4111-1 du Code de la défense :

« La condition militaire recouvre l'ensemble des obligations et des sujétions propres à l'état militaire, ainsi que les garanties et les compensations apportées par la Nation aux militaires. Elle inclut les aspects statutaires, économiques, sociaux et culturels susceptibles d'avoir une influence sur l'attractivité de la profession et des parcours professionnels, le moral et les conditions de vie des militaires et de leurs ayants droit, la situation et l'environnement professionnels des militaires, le soutien aux malades, aux blessés et aux familles, ainsi que les conditions de départ des armées et d'emploi après l'exercice du métier militaire. »

Cette définition est fondamentale car la loi instaure des APNM dont le champ d'action est strictement limité à cette condition militaire. Ces associations, dont les modalités de création et de fonctionnement relèvent du régime des associations régies par la loi du 1^{er} juillet 1901 (en dehors de dispositions spécifiques précisées justement dans la loi de 2015), ont vocation à défendre les intérêts des militaires. Elles sont exclusivement composées de militaires en activité (y compris les réservistes ayant souscrit un contrat à servir dans la réserve) et doivent être ouvertes à tous les corps, tous les grades et toutes les armées ou formations rattachées. Elles doivent avoir une dimension nationale. Ces APNM ont vocation à participer au dialogue avec le commandement à l'échelon national à la condition d'être reconnues comme représentatives. En outre, les APNM représentatives sont appelées à s'exprimer devant le Haut comité d'évaluation de la condition militaire (HCECM).

(1) La notion de « condition militaire » existait déjà dans les textes (articles R. 3121-2 et R. 3121-25 du Code de la défense qui font du CEMA et des CEM les responsables de la condition militaire, et L. 4111-1 sur les compétences du HCECM), mais n'avait pas de définition légale.

Dans son arrêt très attendu de septembre 2016, le Conseil d'État est venu préciser la nature de ces associations *sui generis* que sont les APNM. Comme l'avait indiqué le président Pêcheur ⁽²⁾ dans son rapport, l'interdiction absolue faite aux militaires de se syndiquer ou d'adhérer à une association professionnelle a certes été sanctionnée mais au profit d'une ouverture très limitée. Les APNM ne peuvent nullement être assimilées à des syndicats de droit français (l'article L. 4121-4 du Code de la défense réaffirme que, outre l'interdiction du droit de grève, l'existence de groupements professionnels militaires à caractère syndical est incompatible avec les règles de la discipline militaire). Il s'agit donc en réalité de l'ouverture vers une capacité encadrée de « négociation collective », prise au sens de l'article 11 de la Convention européenne des droits de l'homme (qui doit donc être comprise, non comme le droit à conclure des conventions collectives mais simplement comme le droit au dialogue social avec l'employeur). Les APNM ne peuvent en aucun cas contester la légalité des mesures d'organisation des armées et formations rattachées (Code de la défense, article L. 4126-3).

Les articles R. 4126-1 et R. 4126-2 du Code de la défense rappellent le rôle éminent du ministre de la Défense dans la vérification de la licéité d'une APNM. Il dispose de deux mois, à partir du dépôt des statuts de l'association et de la liste de ses administrateurs, pour vérifier la conformité de son objet. En cas de difficulté, il peut demander la modification des statuts, voire saisir la justice pour demander une dissolution.

Il convient aussi de noter que l'article L. 4111-2 du Code de la défense autorise d'autres associations que les APNM à mener des actions contentieuses contre des actes réglementaires relatifs à la condition des militaires, sous la réserve qu'il n'y ait, à l'inverse des APNM, aucun militaire en activité parmi leurs membres.

La question fondamentale de la représentativité des APNM

Il est évident que la création des APNM pourrait donner lieu à des analyses approfondies, notamment au plan juridique. Le format du présent article ne s'y prête pas mais autorise cependant à évoquer le critère de représentativité, qui apparaît fondamental pour l'existence effective des APNM dans la concertation ⁽³⁾.

On l'a vu, le champ de compétence des APNM est relativement étroit et leur composition doit répondre à des critères spécifiques. À cela se rajoute, pour qu'elles aient la capacité à dialoguer avec les autorités administratives et le commandement au niveau national, la nécessité d'être reconnues comme représentatives. L'arrêté du 21 octobre 2016 est venu préciser ce qui est exigé en la matière, parachevant ainsi la constitution du régime juridique applicable aux APNM. Le texte distingue le cas de la représentativité pour une force armée ou une formation rattachée et le cas d'une APNM souhaitant siéger au CSFM. Nous nous intéresserons plus particulièrement à ce dernier cas qui est de portée interarmées.

(2) Président de la section de l'administration au Conseil d'État et président du Haut comité d'évaluation de la condition militaire (HCECM).

(3) J.-C. VIDELIN, « Représentativité des APNM : dernier acte de la réforme législative », *AJFP*, janvier/février 2017, p. 10.

Tout d'abord, il convient de souligner que toute la structuration des APNM repose sur le statut de ses adhérents ⁽⁴⁾ (exclusivement des militaires en activité) et leur quantité (proportion prédéterminée de l'effectif de la force concernée et des grades en son sein). Cela constitue déjà un élément de rupture avec la situation antérieure où, souvent peu nombreux, les membres des « associations de défense des militaires » étaient avant tout composées d'anciens militaires ou de sympathisants ⁽⁵⁾.

Pour être représentative au CSFM, une APNM :

- doit figurer sur la liste des APNM considérées comme représentatives par le ministre de la Défense ;
- doit disposer d'adhérents issus d'au moins trois forces armées et de deux formations rattachées disposant d'un CFM ;
- doit disposer d'un taux minimal d'adhérents par rapport à l'effectif de chaque groupe de grades dans les formations représentées ;
- doit surtout représenter 2 % de l'effectif total des formations rattachées (ce taux étant ramené provisoirement à 1 % jusqu'au 31 janvier 2021).

Même si ces taux apparaissent faibles en comparaison de ceux exigés par ailleurs pour la représentativité des syndicats ⁽⁶⁾, il faut d'emblée dire que ces critères sont difficiles à atteindre pour les APNM. Le seul moyen pour parvenir à atteindre la cible passe sans doute par un regroupement de certaines APNM par fusion ou fédération, tout en sachant cependant que l'assiette de calcul sera élargie en fonction des entités représentées.

Sans surprise, aucune APNM ⁽⁷⁾ ne remplit aujourd'hui les critères pour être représentative au sein du CSFM (ni même au titre d'une force armée ou d'une formation rattachée d'ailleurs). Cet état de fait, d'abord, révèle que ces APNM (qui, en tant qu'associations, ne disposent pas de moyens alloués) ne sont sans doute pas clairement connues et identifiées pour l'instant par les militaires et, au-delà, pose la question de savoir si la création des APNM correspond ou non à une demande réelle et importante de la communauté militaire. Cela nécessitera une évaluation sur le long terme, d'autant que la question de la déclaration d'adhésion a pu freiner les volontariats.

Un modèle rénové de dialogue social visant l'efficacité

Les instances de concertation nationales ont de fait été réorganisées en profondeur : le CSFM a été redimensionné pour accueillir en son sein les représentants des APNM. Son champ de compétence a été élargi à tous les projets de loi, de décret

(4) La liste des adhérents fait l'objet d'un contrôle par une commission indépendante présidée par un conseiller d'État, dans le respect de l'anonymat.

(5) COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES, *État d'avancement de la manœuvre ressources humaines et les conséquences des arrêts de la Cour européenne des droits de l'homme du 2 octobre 2014 (Rapport d'information n° 2745)*, Assemblée nationale, 6 mai 2015, 144 pages (www.assemblee-nationale.fr/14/rap-info/i2745.asp).

(6) Même si, en réalité, il est difficile de comparer car la représentativité dans le monde civil s'apprécie moins au nombre d'adhérents qu'au nombre de voix obtenues aux élections professionnelles. C'est une originalité des APNM pour lesquelles, hors système d'élections professionnelles, la seule mesure objective de leur audience est leur nombre d'adhérents.

(7) Voir tableau en Annexe.

ou arrêté ayant une incidence sur la condition militaire. Du fait de la multiplication des saisines à venir, cette instance ne fonctionnera plus en deux sessions annuelles mais de façon continue tout au long de l'année, grâce à un nombre de militaires issus des armées réduit, mais de militaires désormais entièrement consacrés à la concertation et déchargés de missions opérationnelles pendant leur mandat. Les CFM sont quant à eux recentrés sur les questions inhérentes à leur métier, propres à chaque armée, et n'étudieront plus systématiquement en première lecture tous les textes soumis au CSFM.

Le nouveau CSFM compte 42 membres en activité représentant les quatre forces armées et 5 formations rattachées disposant d'un CFM, au *pro rata* de leurs effectifs :

- 12 pour l'Armée de terre ;
- 12 pour la Gendarmerie nationale ;
- 6 pour la Marine nationale ;
- 6 pour l'Armée de l'air ;
- 1 pour la Direction générale de l'armement (DGA) ;
- 2 pour le Service de santé des armées (SSA) ;
- 1 pour le Service des essences des armées (SEA) ;
- 1 pour le Service du commissariat des armées (SCA) ;
- 1 pour le Service d'infrastructures de la défense (SID).

Outre ces 42 membres, qui sont élus au sein de leur CFM respectif, 16 sièges, au plus, sont dévolus aux APNM et 3 sièges sont dévolus aux associations de retraités siégeant au Conseil permanent des retraités militaires.

Les membres du CSFM sont répartis en 3 commissions (statuts, rémunérations, conditions de vie et environnement professionnel). Chaque commission se réunit une semaine par mois. Le CSFM se réunit au complet environ une semaine par mois pour rendre les avis officiels. De la sorte, un membre est convoqué à Paris deux semaines par mois. Lorsque les membres ne siègent pas, ils rejoignent leur résidence d'affectation et rendent compte au secrétaire général du CSFM de leur emploi du temps de manière hebdomadaire. Ils ont notamment vocation à visiter les unités militaires implantées dans leur région pour faire remonter les éventuelles préoccupations.

Des imperfections originelles à corriger

Établir des perspectives pour un dispositif neuf qui n'a pas encore été expérimenté serait sans doute présomptueux. En effet, alors même que les APNM n'ont pas subi « l'épreuve du feu », il apparaît difficile de se projeter à la fois sur leur capacité à s'intégrer au dispositif existant et sur leur aptitude à se faire accepter par les personnels en vue de porter une part de leur voix.

Pour autant, il est loisible d'évoquer à ce stade quelques tendances prévisibles et ce qui pourrait être perçu comme des imperfections originelles qui sont de nature à fragiliser le système de concertation dans sa globalité.

Un mode d'action mesuré, clé de l'intégration des APNM

Parmi les APNM naissantes dont les sensibilités seront nécessairement différentes, deux lignes politiques différenciées pourraient rapidement se dessiner : des APNM dont l'objet serait avant tout la contestation à l'égard de l'autorité militaire au nom de la défense des intérêts de certaines catégories de militaires ; *a contrario*, des APNM dont la finalité serait avant tout la défense de la condition militaire, aux côtés de la hiérarchie, en comparaison de la société civile, sans nécessairement dévier vers un militarisme militant et exagéré. Il est clair que la première catégorie d'APNM risque d'emprunter rapidement par mimétisme les modes d'action et d'expression de certains syndicats civils contestataires ⁽⁸⁾ si elles ne sont pas accompagnées et correctement associées. Ces APNM risquent du reste la marginalisation dans une société militaire qui, si elle peut se montrer mécontente, n'est pas séduite par les outrances.

Les militaires souhaitant fonder une APNM gagneraient d'ailleurs à s'inspirer du modèle de l'association du corps préfectoral et hauts fonctionnaires du ministère de l'Intérieur car il s'agit sans doute du modèle de corps qui ressemble le plus au modèle militaire : fortement hiérarchisé, interdit de se syndiquer, disponible et apolitique, le corps préfectoral a su faire émerger une association puissante et reconnue. Des membres du corps de tous grades y tiennent des responsabilités à travers des collèges qui permettent la juste représentation de tous. Les inévitables tensions au sein de l'institution préfectorale (rapports hiérarchiques, contraintes) sont prises en compte au sein de l'association ; cette dernière a par ailleurs vocation à défendre les intérêts du corps préfectoral. Nullement dirigée contre la hiérarchie, l'association est même présidée traditionnellement par un des préfets les plus gradés. C'est dire si son intégration au sein de son administration est réussie.

Une représentation reposant sur un système à demi abouti

Nous l'avons vu, le CSFM se compose aujourd'hui au sein des forces armées d'un mélange hétérogène de membres élus parmi des élus (au sein des CFM de la gendarmerie, du SCA et du SID) et de membres élus parmi des personnels tirés au sort au sein des autres forces et services (six autres CFM). Cet amalgame est issu de la volonté initiale de laisser le choix à toutes les composantes de leur mode de représentation et, disons-le, de ménager la susceptibilité de certains face à un dispositif électif qui aurait été interprété comme le lit d'un syndicalisme rampant. À l'arrivée, le système génère incontestablement un déséquilibre de représentativité qui, de manière inéluctable, s'ajustera dans la durée.

Un autre déséquilibre encore plus profond est lié à l'émergence des APNM au sein du CSFM. La difficulté à faire émerger, sous pression juridique, les associations dans le système a conduit au « mariage de la carpe et du lapin ». Ce point est d'ailleurs extrêmement lié à la question de l'élection, nous y reviendrons. Penchons-nous à

(8) Il convient cependant de souligner que la liberté d'expression reste limitée (on peut d'ailleurs s'interroger sur la portée du devoir de réserve d'un membre d'APNM. Le droit commun doit-il être aménagé ? Et fallait-il laisser cette dimension à la jurisprudence ou la définir dans la loi ?) et que la grève reste bien sûr interdite.

nouveau un instant sur la composition maximale des membres du CFMG : 42 membres issus des CFM, 16 membres maximum pour les APNM et 3 membres pour les retraités. Cela pose clairement la question de la pertinence de l'existence de sièges dévolus à des associations en vertu de leur nombre d'adhérents. En effet, pour être jugée représentative au CSFM il convient de rappeler qu'une APNM doit se prévaloir d'un nombre d'adhérents correspondant à 1 % (2 % après le 31 janvier 2021) des effectifs cumulés (et dans chaque groupe de grades) de trois forces armées et de deux formations rattachées disposant d'un CFM. Cela conduit concrètement aujourd'hui à envisager pour les APNM un premier siège pour 1 750 adhérents, puis 1 siège pour 1 500 adhérents. Objectivement, à l'heure actuelle, ces chiffres semblent hors de portée pour les associations, rendant hypothétique leur présence effective au CSFM dans un premier temps. Cependant, sur le principe et indépendamment de la réalité actuelle, les APNM bénéficient potentiellement d'une surreprésentation. En effet, avec un siège pour 1 750/1 500 adhérents les APNM sont loin du ratio des sièges réservés aux membres issus des CFM avec un siège pour 7 000 à 10 000 personnels représentés selon les forces ou services.

En réalité, ce double écueil (hétérogénéité de la représentation au sein du CSFM et potentielle surreprésentation des APNM) plaide pour un mode électif, plus conforme au modèle démocratique français et, au final, porteur d'autorégulation. Transposons la situation dans un exemple volontairement caricatural : imaginons que les élections des conseillers municipaux dans une commune soient modifiées en raison d'une culture historique du jeu de boules dans la ville. Le conseil municipal est composé de 58 membres qui seront dorénavant répartis de la manière suivante : 42 sièges au suffrage universel direct et 16 sièges réservés à l'association des boulistes de la commune... Il est possible de douter de la représentativité du futur conseil municipal, d'autant que certains des élus au suffrage universel sont peut-être aussi membres de l'association des boulistes sans s'en être prévalu au moment des élections. Une des vertus des élections est de pouvoir mesurer sur un pied d'égalité le poids réel et l'aura des membres, qu'ils soient ou non adhérents des APNM. Un système où les membres seraient tous élus au sein des CFM, puis du CSFM, permettrait d'uniformiser la représentativité, de gommer les quotas réservés aux APNM (le club des boulistes...), de les affranchir dans le même temps des critères de représentativité qui leur sont imposés et qui, paradoxalement, peut conduire à leur surreprésentation. L'exemple de la gendarmerie au CFMG est assez éclairant de ce point de vue. Dans son ancien format, un tiers des 79 membres du CFMG tirés au sort étaient adhérents des APNM. Après l'élection environ 5 membres se réclament des APNM. Ils sont donc présents, élus pour ce qu'ils sont, et dans un volume plus conforme à la réalité. En outre, si les candidats des APNM doivent se présenter parmi leurs pairs lors de l'élection, cela pourrait les amener à adopter un discours moins contestataire (multiples recours administratifs) que celui qui les a pénalisés jusqu'à maintenant. Le but est d'amener les membres des APNM à défendre dans un contexte interministériel des sujets plus consensuels liés à la condition militaire, en abandonnant en interne des querelles intestines où la surenchère est de mise. Il y a fort à parier que les APNM seraient favorables à un système où elles seraient à même de jouer pleinement leur chance, comme dans toute élection, dans le champ de la confrontation mesurée des idées, plutôt qu'un

système qui leur réserve – de manière contestable nous l'avons dit – des places qui semblent surtout virtuelles. En tout cas, ce mode électif aurait pour mérite de contribuer à mieux porter la voix du CSFM dans sa globalité, tant il est vrai que le message vaut avant tout par la légitimité de ceux qui le portent.

La faible place occupée par la représentation militaire dans le champ politique

La communauté militaire interagit aujourd'hui avec de nombreuses entités dans un contexte résolument interministériel et interadministrations. Le dialogue instauré par la communauté militaire doit, dans ce cadre, être proactif et réactif afin de faire valoir de manière efficace son point de vue et gagner en capacité d'influence. De ce point de vue, le système des CFM et du CSFM se montre un peu lourd et peu à même de répondre aux sollicitations. Or celles-ci sont nombreuses car, contrairement à ce que l'on pourrait penser, la sphère politique (terme à envisager ici au sens large) est demandeuse de la représentation militaire. Il ne faut pas se méprendre : il ne s'agit pas ici de prétendre gommer le rôle de la hiérarchie mais, d'évidence, il est des champs où celle-ci n'est pas conviée ou en difficulté pour s'afficher. Comment des chefs peuvent-ils objectivement se montrer dans des cénacles où ils se trouveraient en situation de siéger comme alter ego de certains syndicats de la fonction publique ou répondre à certaines invitations consultatives qui pourraient être interprétées comme partisans au plan politique ? Faire reposer cette catégorie de dialogue sur les seuls chefs revient *de facto* à s'en priver purement et simplement ou à devoir recourir à une forme de clandestinité qui n'est pas dans la nature du militaire qui se prévaut, à raison, d'une droiture et d'une loyauté qui ne peuvent donner lieu au moindre doute.

Aussi, parallèlement au rôle traditionnellement attribué à ses chefs et afin de répondre aux différentes demandes formulées à son endroit, la communauté des militaires de la gendarmerie a doté son outil de représentation naturel qu'est le CFMG d'un groupe de liaison. Ce groupe, dont les membres sont élus pour un an par le CFMG parmi ses propres membres, constitue une structure souple et légère (11 membres) qui est à même de répondre rapidement, en parfaite connaissance de cause, aux diverses demandes, y compris sous court préavis. Petit à petit, ce groupe s'est imposé comme un interlocuteur apprécié des décideurs, à la fois par son sérieux et sa réactivité, bref comme un interlocuteur pertinent, disponible en permanence pour un dialogue respectueux et constructif. Le groupe de liaison du CFMG se trouve ainsi très régulièrement en dialogue avec les décideurs ou des autorités indépendantes. Il en va ainsi, et à titre d'illustration, du ministre de l'Intérieur, du garde des Sceaux, des commissions de l'Assemblée nationale et du Sénat, du Défenseur des droits et du président de la République lui-même.

À l'heure actuelle, hors la gendarmerie, les différents CFM n'ont pas fait le choix de se doter de cette structure légère de liaison et le CSFM non plus. Certes, pour le CSFM, il est prévu l'existence d'un « groupe de contact »⁽⁹⁾. Mais ce groupe de contact ne possède « aucune délégation du conseil et ne peut donc s'exprimer ni

(9) Voir articles 20 à 25 de l'arrêté du 3 octobre 2016 portant règlement intérieur du CSFM et des CFM.

formuler un avis en son nom ». En outre, le seul interlocuteur possible et identifié pour ce groupe de contact est le ministre de la Défense. À l'origine de cette posture se trouve sans doute la volonté de laisser une position incontestée d'intermédiaire à la hiérarchie, ce qui répond à un conformisme historique et au postulat de la représentation affirmée des intérêts des subordonnés par les chefs. Cela peut se défendre et surtout se comprendre. Pour autant, cette attitude est potentiellement porteuse d'effets pervers sur le long terme.

Tout d'abord, l'exemple de la gendarmerie montre que l'existence d'un groupe de liaison susceptible d'« aller au contact » ne prive nullement le commandement de son rôle relationnel privilégié avec les autorités et d'orientation générale des choix institutionnels. Cela est d'autant plus vrai que le commandement reste en lien permanent et très étroit avec le groupe de liaison, et que ce dernier intervient utilement en lieu et place des chefs dans des réunions jugées peu opportunes comme évoqué précédemment, assurant une occupation complémentaire du champ du dialogue social.

Au-delà, c'est la représentativité du CSFM qui est plus particulièrement en question. Si l'on accepte le fait que les décideurs sont demandeurs d'un contact avec la représentation militaire au même titre que d'autres catégories socio-professionnelles, il convient d'être en mesure de répondre aux sollicitations. Le choix s'est porté sur un modèle intégré pour le CSFM, incorporant les APNM en son sein. Ne nous trompons pas : si le CSFM ne se montre pas en capacité de faire entendre sa voix là où le commandement ne peut pas jouer naturellement son rôle ou tout simplement là où les décideurs veulent avoir un contact avec un organisme légitime pour représenter le personnel qui soit distinct des chefs, ce sont les APNM seules qui iront au contact, comme la loi leur en donne parfaitement le droit. C'est l'affaiblissement potentiel du modèle intégré souhaité et, surtout, un risque de déclassement du CSFM avec, au final, une rupture d'équilibre dans la représentation. Une telle évolution serait le terreau de tensions et de querelles intestines qu'il convient de juguler. Autrement dit, il faut que le CSFM se mette en capacité d'occuper le terrain ou il se verra cantonné à un rôle d'aimable groupe de parole...

Conclusion

Les évolutions en cours conduiront les forces armées à envisager des évolutions en matière d'expression et de concertation dans les toutes prochaines années. Rien ne serait pire pour elles que la politique de l'autruche consistant à nier le bien-fondé de la concertation et ses évolutions inéluctables, tout en menant un combat retardateur nécessairement voué à l'échec.

Dans le même temps, il pourrait être souhaitable que le dispositif initial gagne progressivement en cohérence et en légitimité en envisageant, de manière généralisée, la procédure d'élection pour les membres des CFM et du CSFM. Cette posture pourrait également s'envisager pour les membres des APNM, en supprimant les places qui leur sont – en théorie – réservées, au profit d'un débat d'idées apaisé et mesuré dans un cadre électif.

En tout état de cause, il est de loin préférable que les plus hautes autorités militaires s'approprient pleinement à tous les niveaux et dans toutes les forces le changement en cours pour mieux l'accompagner et préserver ainsi les fondements militaires. La cohésion et la discipline militaires n'y perdront alors rien et la condition militaire devrait y gagner.

Éléments de bibliographie

COUR EUROPÉENNE DES DROITS DE L'HOMME, Arrêt du 2 octobre 2014 AFFAIRE MATELLY C. FRANCE (Requête n° 10609/10) ([https://hudoc.echr.coe.int/eng#{"itemid":\["001-146695"\]}](https://hudoc.echr.coe.int/eng#{)).

COUR EUROPÉENNE DES DROITS DE L'HOMME, communiqué de presse relatif à l'interdiction absolue des syndicats au sein de l'armée française contraire à la Convention (Arrêt du 2 octobre 2014 AFFAIRE MATELLY C. FRANCE) (<http://hudoc.echr.coe.int/>).

COUR EUROPÉENNE DES DROITS DE L'HOMME, Arrêt du 2 octobre 2014 AFFAIRE ADEFDROMIL C. FRANCE (Requête n° 32191/09) ([https://hudoc.echr.coe.int/eng#{"itemid":\["001-146700"\]}](https://hudoc.echr.coe.int/eng#{)).

PÊCHEUR Bernard (président de section au Conseil d'État), Rapport à M. le président de la République sur le droit d'association professionnelle des militaires, 18 décembre 2014 (www.ladocumentationfrancaise.fr/).

Loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense, articles 9 à 13 portant dispositions relatives aux associations professionnelles nationales de militaires (et travaux parlementaires avec amendements) (www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030943133&categorieLien=id).

Décret n° 2016-997 du 20 juillet 2016 modifiant diverses dispositions du Code de la défense relatives aux organismes consultatifs et de concertation militaires (www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032922533&categorieLien=id).

Décret n° 2016-1043 du 29 juillet 2016 relatif aux associations professionnelles nationales de militaires (www.legifrance.gouv.fr/eli/decret/2016/7/29/DEFH1609998D/jo/texte).

Arrêté du 12 août 2016 fixant la composition du Conseil supérieur de la fonction militaire et des conseils de la fonction militaire et les modalités de désignation de leurs membres (www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033027781&categorieLien=id).

CONSEIL D'ÉTAT, Arrêt n° 396987, 7^e et 2^e chambres réunies, 26 septembre 2016, ASSOCIATION DE DÉFENSE DES DROITS DES MILITAIRES - AIDE AUX VICTIMES (M^{me} Lévêque, rapp. ; M. Pelissier, rapp. publ.).

Arrêté du 21 octobre 2016 pris en application des articles R. 4126-1 à R. 4126-7 du Code de la défense relatifs aux associations professionnelles nationales de militaires (JORF n° 0263 du 11 novembre 2016) (www.legifrance.gouv.fr/eli/arrete/2016/10/21/DEFH1610000A/jo).

COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES, *État d'avancement de la manœuvre ressources humaines et les conséquences des arrêts de la Cour européenne des droits de l'homme du 2 octobre 2014 (Rapport d'information n° 2745)*, Assemblée nationale, 6 mai 2015, 144 pages (www.assemblee-nationale.fr/14/rap-info/i2745.asp).

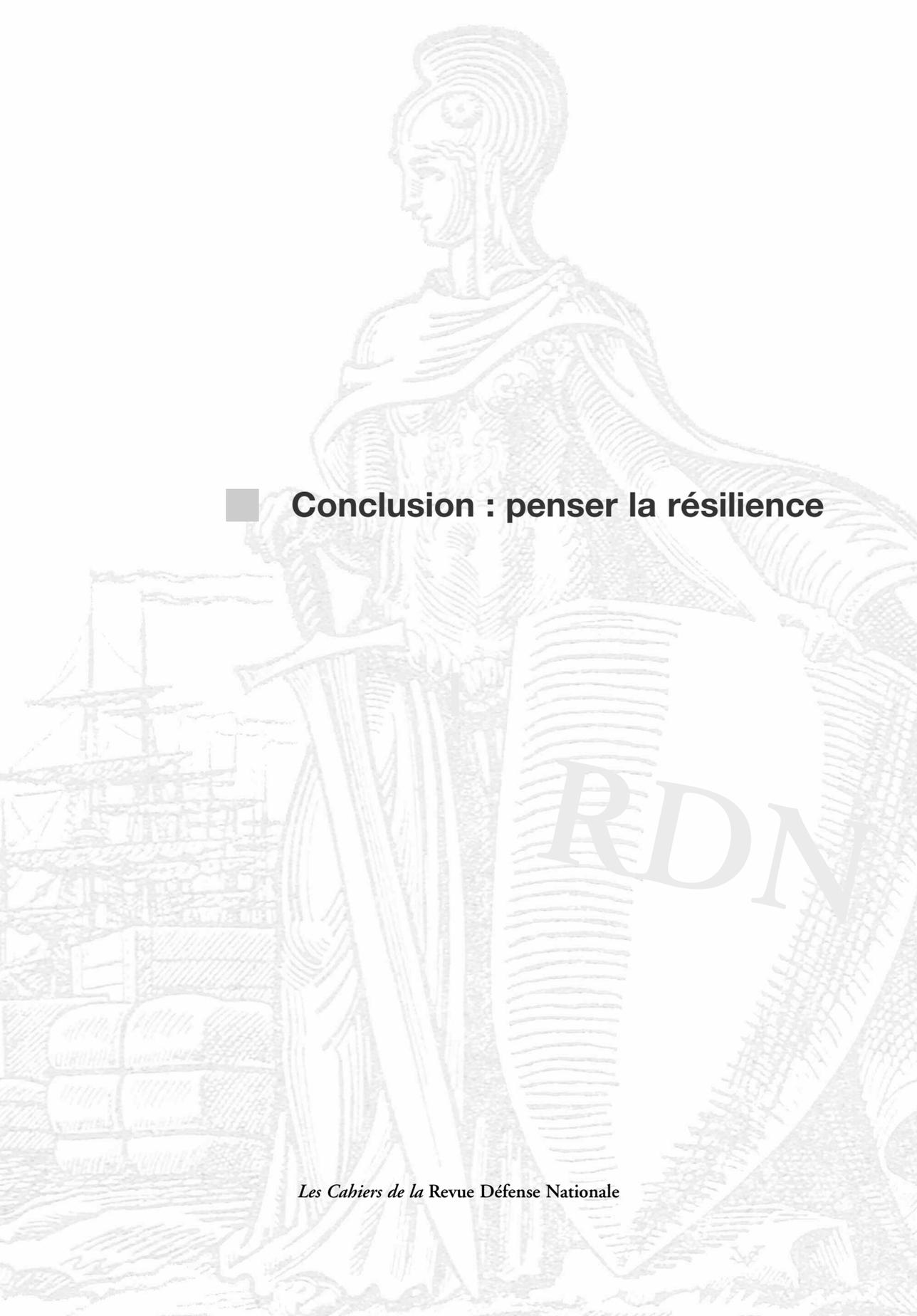
COMBEAU Pascal, « Les associations professionnelles nationales de militaires, et les autres : le Conseil d'État fait le tri », *Actualité Juridique de la Fonction Publique (AJFP)*, janvier/février 2017, p. 7-9

VIDELIN Jean-Christophe, « Représentativité des APNM : dernier acte de la réforme législative, *AJFP*, janvier/février 2017, p. 10-11.

Associations professionnelles nationales de militaires
et dialogue social dans les forces armées

ANNEXE : TABLEAU RÉCAPITULATIF DES APNM AU 31 JANVIER 2017

	Nom de l'association	Abréviation	FAFR représentées	Présidence			Envoi statuts	Réponse DRH-MD
				Grade	NOM	Prénom		
1	GEND XXI	GEND XXI	Gendarmerie	Gendarme	LE LOUETTE	Frédéric	29-sept-15	26-oct-15
2	APNM Marine	APNM Marine	Marine	CV	DE LORGERIL	Dominique	22-janv-16	17-févr-16
3	Association nationale des militaires du XXI ^e siècle	ANM XXI	Marine - SSA	PM	BOUCHE	Jérôme	26-janv-16	17-févr-16
4	Fédération d'associations professionnelles nationales des militaires du XXI ^e siècle	MILI XXI	Fédération	Gendarme	VUILLERMINAZ	Michel	26-janv-16	25-févr-16
5	APNM-Association de défense des droits des militaires et des gendarmes	ADEFDROMIL-GEND	Interarmées	LTN	MORRA	Paul	19-févr-16	29-mars-16
6	Association professionnelle nationale des militaires de l'Air	APNAIR	Air	CNE	HILLAIREAU	Lionel	31-mars-16	11-avr-16
7	Association professionnelle de la Défense	APRODEF	Interarmées	LCL	MOSELE	Jean-Marie	20-avr-16	04-mai-16
8	Association professionnelle nationale des militaires relevant du ministre chargé de la mer	AP3M	Affaires Maritimes	AG (2S)	TOURRET	Georges	07-juin-16	04-juil-16
9	APNM - Commissariat	APNM - Commissariat	SCA	CR1	ANRIJS	Michel	12-juil-16	16-août-16
10	APNM France Armement	France Armement	DGA	ICA	ROBERT	Olivier	17-août-16	06-sept-16
11	Association Gendarmes et Citoyens	AG&C	Gendarmerie	MDL/Chef	GUERRERO	Thierry	12-déc-16	26-janv-17



■ **Conclusion : penser la résilience**

RDN

Le *Pentagone Citoyen*, plaidoyer pour une mobilisation nationale face à un ennemi insaisissable

Cyril CARCY

| Colonel (air), auditeur de la 66^e session du CHEM.

« Il y a dans notre France, sur les problèmes vitaux, une inertie de la pensée, une somnolence de l'esprit qui nous expose à toutes les surprises jusqu'au jour où se produisent ces lumineux réveils qui viennent heureusement, quoiqu'à de trop longs intervalles, sauver notre pays. »

Jean JAURÈS

Depuis les attentats commis par Mohammed Mérah en mars 2012, le terrorisme djihadiste surgit régulièrement et brusquement dans la vie quotidienne des citoyens français. Barbare, sidérant et inique, il provoque, suivant les individus, incompréhension, frayeur ou sentiment de colère voire de vengeance. La déstabilisation généralement observée dans la réaction des Français trouve une double explication : d'une part, par le caractère inaccoutumé du phénomène ; d'autre part, par l'ébranlement des valeurs citoyennes au sein de la société.

Ces opérations terroristes ne devraient pas connaître d'accalmie, voire elles pourraient s'amplifier dans les années à venir eu égard à la nature de la menace. L'ancien ministre de la Défense n'hésitait d'ailleurs pas à parler de « pays en guerre »⁽¹⁾ et évoquait une action sur « le temps long »⁽²⁾. La question est de savoir si un citoyen profondément privé de repères peut encore, en cas de péril majeur, se sentir solidaire de la société au point de résister aux agressions pesant sur ses codes et ses valeurs. Le risque principal réside dans la perte de rationalité de certains de nos concitoyens confrontés à l'effet cumulatif ou insupportable des attentats, qui pourrait conduire à des actions incontrôlées.

L'interdépendance et l'instantanéité, principes sociétaux qui caractériseront notre environnement dans les années à venir, renforcent l'idée qu'il n'y aura de stratégie que globales. L'issue passera par une coordination étroite entre l'ensemble des instruments militaires, sécuritaires, éducatifs, financiers, juridiques et civiques pour instaurer, avec patience, un terrain de sérénité. Cette stratégie inscrite sur le temps long pourrait émerger au travers d'un *Pentagone Citoyen* dont les fondations s'appuieraient sur la mise en synergie des forces vives de la Nation. Les forces de défense, quant à elles,

(1) Jean-Yves LE DRIAN, *Qui est l'ennemi ?*, Éditions du Cerf, 2016, p. 11 : « un pays est en guerre dès lors qu'il n'est plus en mesure de tenir la guerre à distance ».

(2) Jean-Yves LE DRIAN, *op. cit.*, p. 36 : « Il faudra conduire notre action dans le temps long ».

occuperont une place centrale dans cette mobilisation en poursuivant leur action dans la défense de l'avant mais aussi en servant de source d'inspiration voire de repère au cœur d'une société en quête de sens.

La mise en œuvre d'une stratégie globale mue par une impulsion politique passe dans un premier temps par une connaissance précise de l'ennemi contre lequel la France se bat. La projection des enjeux sociétaux à un horizon à dix ans contribuera par la suite à dessiner les contours d'un *Pentagone Citoyen* dont les remparts participeront à entraver l'action terroriste et dont le cœur bénéficiera du concours des forces armées dans de nombreux domaines.

De quel ennemi parle-t-on ?

Dans une analyse des formes récentes de la guerre ⁽³⁾, le sociologue allemand Herfried Münkler précise que la connaissance des faits et de l'ennemi permet de surmonter l'angoisse. Face au terrorisme, la population est d'autant plus vulnérable qu'elle est incapable d'identifier, de situer, de nommer, de rendre visible et intelligible la menace. Ce chapitre est destiné à donner corps à un ennemi invisible et éminemment dangereux.

Un ennemi organisé et hybride

Évoquer *Daech* nécessite de comprendre la stratégie déployée par son chef Abou Bakr Al-Baghdadi. S'affichant comme porteur d'une mission divine, ce dernier s'emploie à diffuser un message ciselé s'appuyant sur une exégèse particulière du Coran. Il peut ainsi s'arroger la puissance divine et devient aux yeux de ses adeptes le Calife, commandeur des musulmans. Cet imam, formé à Bagdad et nommé émir de *Daech* depuis 2010, s'appuie sur une doctrine publiée en 2004 par Abou Bakr Naji, djihadiste égyptien. *Gestion de la barbarie : l'étape la plus importante que franchira la communauté des croyants* ⁽⁴⁾ est un livre prophétisant l'émergence d'un califat né d'actions spectaculaires et de harcèlement destinées à déstabiliser les régimes en place.

Cette doctrine consiste à provoquer le plus de morts possible de manière indiscriminée et à soulever l'ensemble du monde musulman en semant le chaos. Il s'agit d'une perspective eschatologique d'accomplissement de l'histoire qui doit conduire à la conversion ou au ralliement. Appliquée à la France, la stratégie de *Daech* consiste à agir sur notre volonté politique, elle-même fondée sur l'identité nationale. En découlent des lignes d'opérations dont l'objectif est de susciter un sentiment durable de peur au travers d'attentats répétés. Face à une telle menace, les autorités devront déployer des moyens de protection qui s'avéreront insuffisants. Cela conduira à un phénomène de stigmatisation de la communauté musulmane, préalable à l'installation d'un repli communautaire et *in fine* au chaos.

(3) Herfried MÜNKLER, *Les guerres nouvelles*, Éditions Alvik, 2003 ; 256 pages.

(4) L'ouvrage a été traduit et publié en français sous le titre : *Gestion de la Barbarie – L'étape par laquelle l'islam devra passer pour restaurer le califat* (préface de Jacques Heers) ; Éditions de Paris, 2007 ; 250 pages.

Daech incarne ainsi un ennemi organisé qui, de surcroît, s'emploie à exercer son influence dans toutes les dimensions (physique, numérique, perceptive, intime) au gré des circonstances et ce, pour redoubler d'efficacité. Cette asymétrie élargie, que l'on peut qualifier d'hybridité, rend encore plus délicat le combat contre un ennemi aux multiples visages.

Un ennemi qui s'affranchit des règles de la guerre

Le terrorisme djihadiste, qu'il soit affilié à *Daech* ou à d'autres franchises, présente un profil invariant : celui de s'affranchir totalement des normes internationales de la guerre. Ennemi immoral et imprévisible, il a industrialisé l'usage de la barbarie à une échelle culturelle, par la destruction du patrimoine universel, ou militaire, par le recours à une violence extrême et désinhibée. Enfin, il positionne ses centres névralgiques sur des sites protégés par le droit des conflits armés (hôpitaux, écoles, lieux de culte). Il joue ainsi un jeu habile : ses ressources sont préservées face à des adversaires respectueux du droit international et les dommages éventuellement commis à l'encontre des populations civiles sont immédiatement dénoncés pour nourrir la propagande.

En s'employant à mettre en image ses forfaits les plus effrayants, le terrorisme djihadiste maîtrise parfaitement sa politique de communication au service d'une idéologie extrême. La stratégie vise les lignes de faiblesse de nos sociétés (individualisme, communautarisme latent, perte d'identité nationale, peur de la mort...) qui finiront par s'effriter pour fatalement conduire à un retournement des citoyens contre la communauté musulmane sans distinction.

Un ennemi au pouvoir singulier de séduction

La machine d'endoctrinement djihadiste, principalement diffusée sur *Internet*, s'avère sophistiquée tant en qualité qu'en volume. La rhétorique est structurée autour du sentiment d'humiliation et d'exclusion de la société musulmane, érigeant la violence en acte légitime. Il s'agit *in fine* d'une idéologie millénariste et simpliste qui martèle que la construction se fera dans le sang et par la guerre.

Comme l'explique Philippe-Joseph Salazar ⁽⁵⁾, les analogies avec la vie et les paroles du Prophète sont fréquemment utilisées en veillant à proposer une foi simplifiée jusqu'à la caricature et donc très accessible. La séduction s'opère par l'esthétique parfaitement orchestrée de l'image et du son. L'arabe n'est bien souvent pas compris par le spectateur. Cependant, l'exotisme des arabesques et de la calligraphie, l'oreille prêtée au chant choral de la légion califale, la mise en scène du soldat au visage masqué, laissant juste apparaître un regard, sont autant d'éléments lyriques qui participent à la stupéfaction. Ce phénomène de séduction se poursuit par les actes d'égorgement ou de décapitation qui renvoient à une véritable liturgie et à une dimension sacrificielle.

(5) Philippe-Joseph SALAZAR, *Paroles armées, Comprendre et combattre la propagande terroriste*, Éditions Lemieux, 2015 ; 261 pages.

Une telle propagande exploite les frustrations sociales d'une frange vulnérable de citoyens français en rupture familiale, sociale, affective, scolaire ou professionnelle et en quête d'identité. Ces cibles quotidiennes de notre société sont qualifiées de « génération radicale » par le député Malek Boutih dans son rapport éponyme ⁽⁶⁾. Ces jeunes se voient ainsi offrir un rôle correspondant à leurs aspirations. Ils adhèrent « à un projet politique entrant en résonance avec leurs préoccupations internationales et leur rejet de la société démocratique occidentale, plus qu'à une doctrine religieuse fondamentaliste. »

Un ennemi dont l'efficacité bénéficie d'une grande agilité

Ainsi, nos ennemis sont passés maîtres dans la manipulation de nos opinions publiques. Ils utilisent *Internet* car il leur offre une audience à l'échelle mondiale et facilite un changement tactique instantané. *Daech* tient d'ailleurs sa puissance de sa furtivité, de sa capacité à travailler en réseaux et de sa plasticité cybernétique qui lui permet de faire émerger un califat virtuel et de proposer une « cyber-citoyenneté » libre de toute contrainte territoriale.

Quant aux mesures prises pour lutter face aux actions terroristes dans le cyberespace, elles demeurent à ce stade limitées du fait de la nature des réseaux utilisés qui ont la capacité de se dupliquer à l'infini.

La perspective d'une défaite de *Daech* en Syrie et en Irak présage d'un accroissement des actions dans le champ immatériel destinées à stimuler un terrorisme « *low cost* » par le biais des réseaux sociaux. Les messages transmis par l'organisation terroriste pourraient ainsi être entendus et accomplis par une main-d'œuvre « externalisée », désespérée et pléthorique.

*

**

L'ennemi djihadiste présente une dangerosité d'autant plus grande qu'il est structuré, qu'aucune limite morale ne peut entraver son action et que son pouvoir de fascination est mondial grâce à une agilité cybernétique. En outre, la société dans laquelle nous vivons n'étant plus capable de proposer un projet professionnel, social et sociétal, le sentiment d'appartenance à une communauté nationale est très affaibli auprès de nombreux jeunes. Le message diffusé par *Daech* est ainsi parfaitement reçu car il offre une alternative crédible et transcendante à des individus en quête d'espérance.

Enjeux sociétaux prévisibles

Les groupes djihadistes, et *Daech* plus particulièrement, cherchent à fragiliser voire à anéantir le centre de gravité de notre pays, qui n'est autre que la cohésion

(6) Malek BOUTIH, *Génération radicale* (rapport à la demande du Premier ministre, Manuel Valls), juin 2015, 68 pages (www.boutih.fr/wp-content/uploads/2015/07/Génération-radical.pdf).

nationale. La population française est l'objectif militaire sur lequel l'ennemi agit, qu'il s'agisse de l'influencer, la menacer ou l'atteindre. Un tel dessein est d'autant plus aisé que la société présente des fragilités qui, selon toute vraisemblance, devraient poursuivre une trajectoire déclinante dans les dix ans à venir.

Une société vulnérable et en perte de repères

Depuis les années 1950, deux phénomènes se conjuguent avec pour conséquence majeure de dissoudre « l'idéologie » du devoir : d'une part, le développement des droits de l'individu (santé, bien-être, environnement, sexualité, avortement...) et, d'autre part, la légitimation sociale du bonheur et des plaisirs (loisirs, vacances...). Cette société de « l'après-devoir », telle qu'elle a été décrite par Gilles Lipovetsky ⁽⁷⁾, privilégie les désirs immédiats, la passion de l'ego et le bonheur matérialiste au détriment des valeurs collectives.

La société contemporaine voit ainsi l'individu se définir et se réaliser par ce qu'il possède. L'individualisme prend le dessus sur la conscience collective et nationale conduisant à une perte du langage commun. Les médias et les réseaux sociaux exacerbent ce constat alarmant en plaçant l'individu et l'apparence au centre de toutes les attentions. La valeur suprême est devenue la vie de l'individu alors même que le sacrifice de sa vie pour la communauté a été considéré, durant des millénaires, comme un acte de la plus grande noblesse.

La société française est en outre nourrie quotidiennement par un narratif de repentance. Les motifs de fierté et de réussite de la France au fil de son histoire sont rarement mis en exergue ou bien moins que ne le sont les épisodes contestables.

En l'absence de fortes valeurs collectives partagées, de « roman national » distillé autour d'actes de bravoure, la société française perd ses repères. Elle se fissure. Ne parvenant plus à identifier un motif de concorde, elle doute et cherche des refuges de substitution, notamment communautaire.

Une société dont l'environnement futur n'est pas propice à la résilience et à l'unité

Le recours à une projection à 10 ans permet d'éclairer les vulnérabilités sociétales françaises et les faiblesses que l'ennemi n'hésitera pas à exploiter. Le scénario le plus plausible est celui de la confluence d'une urbanisation croissante, d'un vieillissement, *id est* d'un affaiblissement, des populations et d'une exploitation excessive de notre environnement.

La mondialisation se poursuivra au profit d'acteurs transnationaux. L'État continuera à être affaibli par une pression supranationale, qui aura tendance à relativiser sa souveraineté, et à être contesté par un individu autonome, qui cherchera à contourner les règles imposées. La confusion participera à brouiller les modèles traditionnels,

(7) Gilles LIPOVETSKY, *Le Crépuscule du devoir, l'éthique indolore des nouveaux champs démocratiques*, Éditions Gallimard, 1992 ; 300 pages.

comme l'identification d'un ennemi ou la distinction entre une crise intérieure et extérieure, et pourrait fragiliser *in fine* la résilience de la société.

Face à l'urbanisation galopante, l'État pourrait rencontrer des difficultés pour imprimer son empreinte sécuritaire sur certains espaces. Cette vacuité conduirait à l'émergence de communautés géographiques où plus aucune présence étatique n'existerait, terreau de la criminalité et de la radicalisation.

Ainsi, l'analyse prospective met en lumière une société anomique et fragmentée, caractérisée par un délitement des règles sociétales républicaines, leur substitution par d'autres règles et une propension à générer des espaces communautaires en l'absence d'unité nationale, ou des réflexes d'autodéfense dérégulée.

Une société qui demeurera captive des actions dans le champ des perceptions

L'environnement numérique occupera une place grandissante dans le quotidien des individus au point de créer des sources de fragilités. Eu égard à leur addiction à l'information, les opinions seront placées au cœur des enjeux de stratégie. La dimension perceptive sera un enjeu déterminant dans un environnement où l'image et la réputation l'emporteront sur la réalité physique. Les attaques numériques appliquées à une communauté ou une institution pourraient conduire à une vision divergente d'un événement, décrédibilisant la légitimité d'une action.

L'ennemi pourrait en outre s'attaquer à la sphère patrimoniale, symbolisant l'âme d'une Nation au travers de sa culture et de son histoire. Une action parfaitement orchestrée et ciblée pourrait conduire à faire vaciller les convictions d'une Nation ⁽⁸⁾.

Par conséquent, le point de concentration des émotions et des perceptions migrera progressivement au cœur de l'espace numérique. Ce dernier sera à la merci d'une manœuvre globale destinée à faire basculer une crise. L'ambiguïté, l'influence, la duperie, la manipulation et la désinformation seront autant de procédés utiles pour agir sur les individus, les communautés voire les institutions.

Face à un ennemi déterminé à exploiter nos failles sociétales

Quand bien même le champ d'affrontement pourrait évoluer d'ici une dizaine d'années, le terrorisme djihadiste conservera le même dessein : celui de surprendre pour sidérer mais aussi celui de pénétrer pour mieux essaimer. Les modes d'action exploiteront les failles endémiques de notre société comme celles liées à l'identité nationale, à la résistance au sens large et à l'absence de perspectives.

Le terroriste continuera à faire preuve d'une détermination sans faille guidée par une vision eschatologique de l'Islam. À l'opposé, la société pâtira non seulement de ses fragilités organiques et pourra difficilement compter sur les autorités politiques inhibées face aux décisions à prendre sur des sujets sociaux sensibles (religion, laïcité,

(8) Exemple récent : arrestation à Montpellier le 10 février 2017 d'un commando de 3 personnes prévoyant de frapper la Tour Eiffel pour « marquer les esprits ».

appartenance ethnique...). Cette incapacité à mobiliser restera handicapée par la dictature du temps médiatique : face à l'horreur, l'émotion continuera à prendre le pas sur le rationnel, qui privilégierait des réponses s'inscrivant sur le long terme.

*
**

Les confrontations demeureront l'affrontement des volontés. Le déficit prégnant entre une société civile désenchantée et faible, faisant face à un ennemi fanatisé et aguerri ne laisse que peu d'espoir sur l'issue de la bataille. Ainsi, une armée de fanatiques, persuadés d'incarner la vérité, pourrait mettre en échec le bloc national si aucune stratégie n'est mise en œuvre.

Proposition d'approche globale : le *Pentagone Citoyen*

Face à une augmentation prévisible des attentats en France, la demande de sécurité de la part de la population restera forte. Comme le rappelle le précédent président des États-Unis, la lutte contre le terrorisme doit s'inscrire sur le long terme : « On ne vainc pas le terrorisme, on ne vainc pas un mode d'action, on le combat, on le fragilise, on le limite. La victoire sera ailleurs, sur le long terme. »⁽⁹⁾.

Une telle persévérance s'explique par le fait qu'il est difficile de détruire une idée. Face aux attaques cinétiques, l'idéologie djihadiste survivra et mutera sans cesse. Il s'agit donc de penser au-delà des seuls effets militaires et d'adopter une approche globale fondée sur l'éloge de la nation. Les armées pourront jouer un rôle clé dans cette stratégie eu égard à leur longue expérience dans la lutte contre le terrorisme et aux valeurs qu'elles incarnent.

Une impulsion politique pour une stratégie interministérielle

Le nouveau plan Vigipirate, adopté en conseil de Défense restreint de décembre 2016, est accompagné d'un document élaboré par le SGDSN intitulé : *Vigipirate – Faire face ensemble*. Ce plan de sensibilisation est destiné à faire en sorte que chaque citoyen devienne un acteur de la sécurité. Au travers de simples conseils comportementaux, les individus sont encouragés à développer une conscience raisonnée des événements leur permettant d'acquérir une juste perception des dangers.

Toutefois, si les individus perçoivent progressivement la menace, ils n'ont pas ou peu conscience de la capacité collective de résister. En tentant de définir la Nation, Ernest Renan évoquait un lieu dans lequel les hommes doivent « avoir souffert, joui et espéré ensemble »⁽¹⁰⁾. Ainsi, à l'heure où la société française est vulnérable, apeurée et en proie à des fissures communautaires, elle doit être rassurée et stimulée par une initiative politique.

(9) Discours de Barack OBAMA cité par Scoott WILSON et AL KAMEN, « 'Global War On Terror' is given new name », *Washington Post*, 25 mars 2009 (www.washingtonpost.com/wp-dyn/content/article/2009/03/24/AR2009032402818.html).

(10) Conférence prononcée par Ernest RENAN, « Qu'est-ce qu'une Nation ? », Paris-La Sorbonne, 11 mars 1882.

Les forces armées et de sécurité intérieure sont fortement sollicitées. La capacité à durer est d'ores et déjà ébranlée, hypothéquant largement la sécurité de la population face à une menace croissante. Il est donc temps d'agir, évitant ainsi d'attendre le prochain « Bataclan », en commençant une impulsion politique qui puisse résonner dans la conscience de chaque citoyen.

Prenant exemple sur les pratiques démocratiques athéniennes, cette annonce présidentielle pourrait prendre la forme d'un « Appel à la Nation », à l'instar de celui du 18 juin 1940, pour encourager à un nouveau choix de société et convaincre chaque individu à prendre ses responsabilités. Un plan stratégique interministériel serait associé, validé par le parlement réuni en Congrès. Il ferait par la suite l'objet d'un suivi centralisé par un ministère dédié.

Au cœur d'une Cité déterminée à faire face et à résister

L'ennemi connaît d'autant plus les faiblesses de la Cité qu'il y vit au quotidien. La société est certes la cible à frapper mais elle peut également devenir la meilleure arme à opposer à *Daech*.

L'époque de la levée en masse, permise par la conscription, est révolue. Chaque citoyen doit donc acquérir progressivement un état d'esprit et un comportement lui permettant d'être relié à la collectivité dont il partage le destin. Pour donner corps et sens à cet « esprit de défense », chaque Français doit adopter des attitudes conformes au droit mais aussi aux devoirs. Plus délicat, il devra prendre conscience de son rôle dans la société et s'engager dans l'intérêt collectif.

En somme, il s'agit de prendre exemple sur la société suisse dont le fonctionnement se fonde sur le modèle de la démocratie athénienne. Chaque individu se considère comme un citoyen en armes. Parce qu'il n'y a pas de liberté sans devoir, sans abnégation et sans sens du collectif, c'est en assurant sa propre défense que chaque Suisse gagne le droit de participer à la vie de la cité.

Le Pentagone citoyen : une mobilisation volontariste et inscrite sur le long terme

Une fois l'impulsion politique donnée, la mise en œuvre du plan gouvernemental pourrait être confiée à un ministère de la « communication et de la cohésion sociale », comme le suggère le député Malek Boutih dans son rapport. Quant aux fondations de cette stratégie globale, elle pourrait s'appuyer sur un Pentagone citoyen associant l'Éducation nationale, les communautés religieuses, les relais et faiseurs d'opinion ⁽¹¹⁾, les citoyens et les forces de sécurité intérieure.

L'Éducation nationale doit principalement inscrire son effort dans le renforcement du savoir-être auprès des élèves. Il s'agit également de transformer les questions de défense et de sécurité en champs disciplinaires d'enseignement, favorisant ainsi l'acquisition d'un esprit de défense. Le réseau « Espérance Banlieues », créé en 2012,

(11) Élus, médias, milieux intellectuels, acteurs d'*Internet* (Google, Facebook, Twitter...).

incarne parfaitement cette mission. La recette s'appuie sur trois piliers : la responsabilisation des parents ; la transmission des valeurs nationales ; et la connaissance de notre pays au travers de sa langue, de sa culture et de son histoire. Les résultats sont tangibles au point d'approcher la quinzaine d'établissements ouverts à compter de la rentrée prochaine.

La contribution des *communautés religieuses* doit s'inscrire dans la continuité de celle de l'Éducation nationale en centrant leur effort sur l'adhésion aux valeurs de respect, de responsabilité et de solidarité prônées par chacune des religions monothéistes. Un dialogue inter-religieux régulier participera également à cette connaissance mutuelle.

Les *relais et faiseurs d'opinion* ont un rôle structurant dans cette entreprise. Pour contrer le discours djihadiste, qui séduit une jeunesse en manque de repères et de perspectives, il est nécessaire de substituer le discours de victimisation en faveur d'un contre-narratif d'héroïsation. L'effort consisterait simplement à conter l'histoire de héros nationaux ou à valoriser de simples citoyens dans leurs actions quotidiennes. Les acteurs d'*Internet* pourraient apporter leur soutien à cette stratégie, comme ils le font déjà outre-atlantique au travers de l'initiative *Global Engagement Center (GEC)*. Cette agence interministérielle américaine, créée en 2016, permet de rediriger habilement les internautes, souhaitant s'informer sur les sites djihadistes, vers des vidéos condamnant les groupes terroristes.

Les *citoyens* doivent jouer le rôle de passerelle et d'éducateur auprès des plus jeunes. Le vide laissé par la suspension de la conscription, comme facteur d'intégration, est palpable. Le propos n'est pas de blâmer cette décision politique mais de pallier cette carence au travers d'un engagement sans relâche. La Journée défense et citoyenneté (JDC) est insuffisante pour sensibiliser les individus âgés de 16 à 25 ans qui y participent. Les parents, amis et voisins peuvent jouer le rôle de relais pour encourager les jeunes à inscrire leur empreinte sociétale dans le champ des idées, des comportements et des valeurs.

Les *forces de sécurité intérieure*, enfin, occupent une place cardinale dans ce Pentagone car elles apportent leur contribution dans les champs sécuritaires et judiciaires. Cependant, le rythme d'emploi qu'elles connaissent actuellement ne faiblira pas au risque d'épuiser les unités de police et de gendarmerie. En outre, l'ennemi pourrait décider de durcir ses modes opératoires (attaques multiples, usage de moyens NRBC ⁽¹²⁾...), conduisant à une saturation des éléments d'intervention. Autant de perspectives prévisibles militent pour le maintien de l'opération *Sentinelle*. Cette dernière devra dans ce cas poursuivre sa dynamique d'adaptation en prenant soin de renforcer l'interopérabilité entre forces des ministères de la Défense et de l'Intérieur. Il existe du reste de nombreux champs à défricher pour parvenir à une synergie parfaite : l'aéromobilité, le partage du renseignement, l'emploi de systèmes de drones militaires, les SIC ⁽¹³⁾, la cyberdéfense, le soutien logistique et l'échange de savoir-faire précieux acquis sur les théâtres d'opération (déménagement d'explosifs artisanaux, NRBC...).

(12) Nucléaire, Radiologique, Bactériologique, Chimique.

(13) Systèmes d'information et de communication.

En plaçant les Armées au centre de la mobilisation

L'exemple précédent de coopération entre les unités militaires et celles de sécurité intérieure peut être généralisé à bien d'autres contributions au profit de la collectivité. En 1891, le maréchal Lyautey exhortait les officiers à embrasser un rôle d'éducateur de la Nation. Il écrivait dans la *Revue des deux mondes* : « car l'armée resterait toujours la meilleure, sinon la seule école où s'apprendront les vertus de discipline, de respect et d'abnégation »⁽¹⁴⁾.

Les sondages réalisés auprès de la population mettent en évidence une admiration des Français pour leur armée. Quatre raisons principales traduisent ce sentiment de fierté :

- L'institution a conservé des valeurs solides au cœur d'une société égarée : humanité, ascenseur social, solidarité, équité, discipline, dépassement de soi, justice, courage.
- La France a peur et souhaite être rassurée par une communauté dont la résilience et la force morale participent à une perception rationnelle de la situation.
- Les forces armées sont dépositaires d'un engagement sans faille et conservent une capacité à fonctionner dans des environnements très dégradés.
- Les militaires sont l'émanation de la Nation. Ils incarnent les valeurs de notre pays et l'espérance de la jeunesse française au service de la paix.

En somme, les forces armées sont perçues comme un phare au cœur de la tempête, un repère dans le brouillard d'une existence sans perspectives. Elles apportent une contribution significative au « principe de réalité » décrit par les psychanalystes comme un régulateur du fonctionnement psychique, détournant les individus des plaisirs et des pulsions pour admettre l'existence de la réalité. Ce sont donc autant de leviers sociétaux et sociaux qui méritent d'être exploités en plaçant les armées au cœur du *Pentagone Citoyen*. Les différents acteurs de cette mobilisation nationale pourraient ainsi graviter autour d'un noyau à la fois rassurant, régénérant et stimulant.

Quant aux interactions concrètes envisageables, elles existent déjà à dose homéopathique et pourraient être étendues tout en veillant à préserver les effectifs militaires fortement engagés. À titre de spicilège non exhaustif, les pistes ci-dessous pourront servir de base à une dynamique vertueuse en gardant à l'esprit la nécessité d'inscrire le combat sur le terrain des valeurs, pivot de cet engagement contre un ennemi insaisissable, au cœur d'une société en quête de sens.

Dans la perspective de générer un terreau favorable, l'Éducation nationale est bien entendu l'acteur à servir en premier. Les initiatives suivantes méritent d'être explorées :

- Engagement systématique des sous-officiers supérieurs et des officiers des armées dans la réserve citoyenne de l'Éducation nationale.

(14) Hubert LYAUTEY, « Du rôle social de l'officier dans le service universel », *Revue des deux mondes*, mars 1891.

- Revitalisation du parcours citoyen JDC en s'appuyant sur le trinôme académique ⁽¹⁵⁾ et l'association Cidan ⁽¹⁶⁾. L'effort consisterait à renforcer, dès la classe de 4^e, l'enseignement sous la forme de modules annuels « défense ». Les actions en faveur du « devoir de mémoire » devront également être renforcées.

- Rattachement du réseau Espérance Banlieues à l'enseignement privé sous contrat, moyennant quelques dérogations au respect des programmes, eu égard au fonctionnement singulier et, pour le moins efficace, de la Fondation.

- Rapprochement des différents dispositifs d'insertion socio-professionnelle (SMA, Épide, SMV ⁽¹⁷⁾) dans un souci d'échanges de bonnes pratiques.

- Formation et emploi des jeunes issus des organismes d'insertion professionnelle précédemment décrits en renfort des unités militaires dans des missions basiques (logistique, filtrage, surveillance...).

Les *communautés religieuses* pourraient utilement profiter de l'expérience insolite acquise par les aumôniers militaires qui côtoient et accompagnent les hommes et les femmes des armées dans des environnements défigurés par les combats. Face à ces ravages physiques et moraux, ces représentants du culte ont appris à cultiver les valeurs les plus nobles de respect, d'humilité et de solidarité.

Les *relais et faiseurs d'opinion*, quant à eux, joueraient un rôle de caisse de résonance du message délivré par les quatre autres acteurs. Les forces armées pourraient, quant à elles, offrir leur contribution au travers de deux axes principaux :

- Celui de l'héroïsation, synonyme d'espérance et de perspectives, en mettant en scène des jeunes militaires, issus de banlieues sensibles, totalement épanouis et fiers du sens qu'ils donnent à leur mission de protection des citoyens français.

- Celui des valeurs incarnées par les militaires, qui pourraient servir d'exemple et élever les citoyens dans leur quotidien, comme celles de la fraternité d'armes, du courage, du dépassement de soi et de la responsabilité.

Les *citoyens*, enfin, ont un rôle essentiel à jouer dans la montée en puissance de la Garde nationale. Créée après l'attentat de Nice, cette institution a pour vocation de renforcer l'Armée, la Gendarmerie nationale et la Police nationale par des volontaires servant au titre d'un contrat d'engagement dans la réserve opérationnelle. L'objectif est de déployer 9 250 réservistes à l'horizon 2018, avec un objectif à 85 000 inscrits ⁽¹⁸⁾. Les armées auraient en outre intérêt à développer l'initiative de « réserve inversée », lancée par l'Armée de l'air, consistant à proposer aux entreprises les services de militaires une vingtaine de jours par an. Cette démarche présenterait l'avantage de partager les bonnes pratiques et de transmettre l'état d'esprit et les valeurs spécifiques aux armées.

(15) Convention cadre entre l'Éducation nationale, la Défense et l'IHEDN.

(16) Civisme défense Armée Nation.

(17) SMA : Service militaire adapté (au profit des jeunes en outre-mer) ; Épide : Établissement pour l'insertion dans l'emploi ; SMV : Service militaire volontaire (au profit des jeunes en métropole).

(18) Les réserves opérationnelles de la Police, de la Gendarmerie et des Armées représentent actuellement un vivier de 63 000 personnes dont 5 500 employées chaque jour.

*

**

Les armées ne sont plus une institution intégratrice comme elles ont pu l'être au temps de la conscription. Cependant, elles peuvent encore jouer le rôle de fédérateur et d'éclaireur dans une société fragmentée et désincarnée. En faisant en sorte que les jeunes recrues militaires d'active comme de réserve deviennent des hommes et femmes responsables et courageux, les armées occuperont une place centrale dans le redressement de la Nation.

Conclusion

Depuis 2012, la France a connu une vague d'attentats djihadistes d'un nouveau genre. L'ennemi auquel elle est confrontée est jeune, agile, déterminé et sanguinaire. Il vit tapi dans l'ombre, au cœur de la cité. Fanatisé par une propagande aiguïlée, il peut frapper à tout moment. Son intention est de sidérer par des exactions insoutenables pour susciter le chaos.

Le terrorisme islamiste cherche ainsi à fissurer la cohésion nationale. Connaissant parfaitement les maux de la société, il profite de l'étiollement des valeurs citoyennes élémentaires et se développe sur le terrain de la désespérance. Les images, l'émotion et la morale réduite à l'indignation et aux bons sentiments sont devenus les modes d'expression d'une société qui a perdu le sens du tragique et de l'histoire. Les individus sont persuadés de vivre à l'abri des désordres du monde, témoignant ainsi de leur cécité face au péril djihadiste.

Il s'agit donc de remettre en cause cette illusion avant que le barbare ne triomphe face à un citoyen qui se serait déjà rendu, trop apeuré pour lui résister. Seule une stratégie globale, mue par une impulsion politique, participera à rendre la société plus résiliente, à défaut d'éradiquer la menace. Elle s'appuiera en outre sur un ensemble cohérent de leviers sociétaux et devra s'inscrire sur le long terme.

La force de l'Homme réside dans le langage. Il s'agit du premier organe de régulation en démocratie, lequel contribue à réduire les conflits grâce au dialogue. La société de « l'après-devoir » actuelle évolue dans un environnement où le langage commun a fait place à différents dialectes. Cette cacophonie ambiante génère une dégradation des valeurs communes et un progressif repli communautaire.

Dans son *Histoire de la guerre du Péloponnèse*, Thucydide affirmait que « la force de la Cité ne réside ni dans ses remparts, ni dans ses vaisseaux, mais dans ses citoyens et leur hauteur d'âme »⁽¹⁹⁾. La restauration d'un idiome compréhensible par tous et d'un état d'esprit combatif pourrait utilement s'appuyer sur l'instauration d'un *Pentagone citoyen*, initiative stratégique associant les principaux acteurs de la vie de la cité. Quant à la rhétorique la plus adaptée à cette entreprise, elle devra s'appuyer sur le « roman national », celui de la fierté légitime que la France peut afficher au titre de la place

(19) THUCYDIDE, *Histoire de la Guerre du Péloponnèse – Tome II*, Éditions Flammarion, 1993 ; 310 pages.

qu'elle a tenue dans l'histoire du monde, aussi bien que de ses réalisations actuelles, et des ambitions dont elle est porteuse.

Au travers de leurs traditions, les forces armées honorent le patrimoine national édifié par une somme de sacrifices qui donne le vertige. Les armées sont l'émanation de la société et ont la capacité à fonctionner dans des environnements très dégradés. Elles portent le fer à l'extérieur du pays et combattent les djihadistes en Afrique et au Levant tout en dissuadant, dans le même temps, les potentiels terroristes sur le territoire métropolitain grâce à la force *Sentinelle*. Enfin, elles incarnent des valeurs solides et éprouvées, syntaxes nécessaires pour recouvrir un langage national.

Dans le cadre du cycle pédagogique, un professeur d'histoire d'un établissement scolaire issu du réseau « Espérance Banlieues » a souhaité faire découvrir aux classes de 3^e les plages du débarquement. C'est au cours d'un de ces déplacements que le jeune Mohammed a assisté fortuitement à une cérémonie militaire commémorant la fusillade par les Allemands d'un jeune résistant de 18 ans. À l'issue de la cérémonie, l'élève de 14 ans est allé voir son professeur. Il lui a confessé avoir bien mieux compris l'enseignement dispensé au cours de l'année. Ému, il a ajouté : « Cette France-là, nous aussi, on peut l'aimer ! ».

Le Pentagone Citoyen, plaidoyer pour une mobilisation nationale face à un ennemi insaisissable

Éléments de bibliographie

BOUTIH Malek, *Génération radicale* (rapport à la demande du Premier ministre, Manuel Valls), juin 2015, 68 pages (www.boutih.fr/wp-content/uploads/2015/07/Génération-radical.pdf).

CICDE, *Environnement opérationnel futur, réflexion de prospective interarmées (RPIA n° 2016/001)*, 2016.

COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES, Audition du général Poncelin de Raucourt (secrétaire général de la Garde nationale et du Conseil supérieur de la réserve militaire), Assemblée nationale, 16 novembre 2016 (www.assemblee-nationale.fr/14/cr-cdef/16-17/c1617016.asp).

COURRÈGES D'USTOU (DE) Bernard (dir.), *EspritS de défense*, IHEDN, 2016 ; 174 pages (www.ihedn.fr/sites/default/files/atoms/files/ihedn_esprits_de_dc3a9fense_2015_0.pdf).

EULRIET Irène (dir.), *Le rôle social des armées : perspectives comparatives et actualité*, *Laboratoire de l'Irsem* n° 12, 2012 ; 105 pages.

LE DRIAN Jean-Yves, *Qui est l'ennemi ?*, Éditions du Cerf, 2016 ; 80 pages.

LIPOVETSKY Gilles, *Le Crépuscule du devoir, l'éthique indolore des nouveaux champs démocratiques*, Éditions Gallimard, 1992 ; 292 pages

MÜNKLER Herfried, *Les guerres nouvelles*, Éditions Alvik, 2003 ; 256 pages.

RENAN Ernest, Conférence « Qu'est-ce qu'une Nation ? », Paris-La Sorbonne, 11 mars 1882.

SALAZAR Philippe-Joseph, *Paroles armées, Comprendre et combattre la propagande terroriste*, Éditions Lemieux, 2015 ; 261 pages.

SERVENT Pierre, *Extension du domaine de la guerre*, Éditions Robert Laffont, 2016 ; 306 pages.

SGDSN, *Vigipirate, Faire Face Ensemble, Vigilance, Prévention et Protection face à la menace terroriste*, décembre 2016, 76 pages (www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd_0.pdf)

THUCYDIDE, *Histoire de la Guerre du Péloponnèse – Tome II*, Éditions Flammarion, 1993 ; 310 pages.

WILSON Scoott et AL KAMEN, « 'Global War On Terror' is given new name », *Washington Post*, 25 mars 2009 (www.washingtonpost.com/wp-dyn/content/article/2009/03/24/AR2009032402818.html).

Entretiens

- Général (2S) Vincent LAFONTAINE, Fondation « Espérance Banlieues ».
- M^{me} Hayette HAMIDI, Association « France Fièrè ».
- M. Alain BAUER, Professeur de criminologie.
- M^{me} Anne JOUAN, Journaliste au *Figaro*, spécialiste du terrorisme.

Penser demain

66^e session du Centre des hautes études militaires

Le Centre des hautes études militaires (CHEM) prépare chaque année 30 auditeurs français et étrangers, du grade de colonel, capitaine de vaisseau ou équivalent, aux hautes responsabilités qui leur seront confiées ensuite, en consolidant leurs qualités personnelles de chef et de cadre dirigeant, en complétant leurs connaissances du fonctionnement de l'État, du ministère et de l'environnement de la défense, des relations internationales et en développant leur compréhension de la relation politico-militaire.

Les meilleurs d'entre eux ont vocation à armer dans dix ans les postes sommitaux de la hiérarchie militaire. Cette année de réflexion et d'étude au CHEM a été l'occasion de se projeter à cet horizon. Invité à « Penser demain », chacun a ainsi réalisé une étude prospective, dont quelques-unes sont proposées à votre lecture dans ce *Cahier de la Revue Défense Nationale*.

Leurs réflexions ont tourné autour de quatre thématiques :

- Penser la défense de l'Europe.
- Penser les opérations.
- Penser les évolutions technologiques.
- Penser le soutien.



Lancée en 1939 par le Comité d'études de défense nationale (Association loi 1901), la *Revue Défense Nationale* assure depuis lors la diffusion d'idées nouvelles sur les grandes questions nationales et internationales qu'elle aborde sous l'angle de la sécurité et de la défense. Son indépendance éditoriale lui permet de participer activement au renouvellement du débat stratégique. La *Revue Défense Nationale* permet de garder le contact avec le monde de la défense et apporte, grâce à ses analyses, la réflexion à l'homme d'action.