

Revue Défense Nationale

Juin 2012 - n° 751

***Eurosatory* - L'Armée de terre face à ses missions**

Bertrand Ract Madoux

La Chine, le nouveau « Péril jaune »

Pierre Conesa

La sécurité maritime mondiale

Patrick Boissier

Cyberstratégie

Jean-Marie Bockel, Daniel Ventre, Olivier Kempf,
Loïc Simonet, Vincent Joubert, Sébastien Héon,
François Géré, Sébastien Gourtay

Le dilemme syrien du *Hezbollah*

Jean-Loup Samaan

Le *New START Treaty*

Steven Ekovich

L'universalisme occidental

Nicolas Tenzer





Éditorial

C'est le mois d'Eurosatory, comme tous les deux ans. Cette année, c'est également le mois où commence une nouvelle législature avec un Parlement renouvelé dont la mise en place va clore un long épisode politique. Beaucoup de préoccupations de défense viennent à l'esprit en ce mois de juin : la transition afghane, l'effervescence sahélienne, l'Europe militaire, la Russie poutinienne, la défense antimissile et la cyberdéfense et, comme cela a été dit ces derniers mois, bien entendu, la croissance économique et la contrainte budgétaire.

Eurosatory offre une occasion de se pencher sur les leçons opérationnelles apprises sur le terrain d'engagements récents, sur les innovations technologiques sorties des laboratoires des industriels ⁽¹⁾, sur l'évolution des conditions du combat terrestre, sur ce que les forces armées doivent être capables aujourd'hui d'accomplir au sol. C'est un rendez-vous essentiel pour faire un point militaire et prendre une meilleure conscience des convergences nécessaires pour consolider cette base industrielle et technologique européenne sans laquelle il est difficile d'asseoir un projet de sécurité commune et de réelle communauté de destin.

Dans le paysage stratégique, dessiné en 2008 par le *Livre blanc* et qui sera réévalué prochainement, il y a l'attention à la vulnérabilité cybernétique de la France ⁽²⁾ qui constitue pour beaucoup une priorité dépassant la protection antimissile de notre pays et de l'Europe. Cette nouvelle approche de la défense et de la sécurité par la réduction résolue de nos vulnérabilités intrinsèques, plutôt que par l'engagement de menaces devenues trop diffuses pour être contrées, marque d'ailleurs un tournant décisif dans notre posture stratégique. Elle pourrait servir de fil conducteur aux nécessaires entreprises de la sécurité européenne.

Aux bénéfices que nous tirons de la mondialisation, trop vite dénoncée alors qu'elle nous permet de garder une prospérité, certes en berne mais enviable au 5^e rang de l'économie mondiale, sont associées de nouvelles dépendances qui sont autant de vulnérabilités que nous partageons avec nos voisins européens et maghrébins : les domaines cybernétiques, spatiaux, maritimes sont devenus vitaux pour nos libertés. Il faut donc les contrôler et les défendre avec résolution, leur affecter des moyens humains et techniques suffisants et nous organiser collectivement pour faire face à ces nouveaux enjeux transversaux de la sécurité du pays. Ce sont eux les vrais vecteurs de la précarité stratégique de la France du XXI^e siècle beaucoup plus que l'évolution heurtée de voisinages à l'Est ou au Sud de l'Europe, avec lesquels nous composons nos destins depuis des siècles. Avec eux, une coopération confiante est un objectif à notre portée si nous savons sortir d'un occidentalisme défensif et promouvoir avec méthode un vaste espace stratégique stabilisé de l'Atlantique à l'Oural et du Cap Nord au Sahel.

Voilà une feuille de route possible et une perspective stratégique de moyen terme pour éclairer une législature qui commence dans le brouillard économique.

Jean Dufourcq - *Rédacteur en chef*

(1) Voir les réflexions publiées à l'occasion d'Eurosatory en coopération avec *Theatrum belli*, p. 8.

(2) Voir le dossier complémentaire de réflexions approfondies sur ce thème, p. 7.

Sommaire

JUIN 2012

9 *Eurosatory* - **L'Armée de terre face à ses missions**

BERTRAND RACT MADOUX

Héritière de choix technico-opérationnels faits il y a quinze ans, forte d'une préparation opérationnelle soignée et d'une adaptation réactive conduite par l'expérience de nombreux et durs combats, l'Armée de terre est un outil polyvalent et réversible dont la cohérence et l'adaptabilité restent l'un des principaux soucis du général qui en est le chef d'état-major.

13 *Préambule* - **La Chine, le nouveau « Péril jaune »**

PIERRE CONESA

En démontant la construction dynamique qui fait de la Chine un ennemi convenable pour rassembler la communauté occidentale, l'auteur dévoile une autre Chine qu'il faut encourager à renforcer la communauté internationale et à prendre une part constructive de la gouvernance mondiale.

19 *Avant-propos* - **Enjeux et perspectives de la sécurité maritime mondiale**

PATRICK BOISSIER

Le développement des flux de la mondialisation a comme support principal les océans. Il dépend étroitement de la sûreté des activités qui s'y développent, soit pour y commercer, soit pour en exploiter des richesses qui relaient de plus en plus celles produites à terre. La France, acteur naval historique, a des capacités importantes à faire valoir pour participer à une gouvernance maritime en plein développement.

Cyberstratégie

27 **La cyberdéfense**

JEAN-MARIE BOCKEL

C'est à une prise de conscience générale de la vulnérabilité des activités informationnelles du pays que l'auteur, rapporteur du Sénat sur la question, invite. Des déconvenues récentes, la comparaison avec nos partenaires, le lent démarrage de notre posture de sécurité cybernétique le conduisent à préconiser de renforcer résolument la cyberdéfense de la France.

33 **Le cyberspace : définitions, représentations**

DANIEL VENTRE

En partant des représentations possibles du cyberspace, on peut mesurer l'importance et la variété des domaines qu'il recouvre. En entreprenant de le modéliser par un système multicouches, on comprend mieux en quoi c'est un espace de combat et un champ d'une bataille transversale qui affecte tous les espaces d'engagement.

39 **Cadre de recherche de la cyberstratégie**

OLIVIER KEMPF

Dans cette large réflexion typologique à valeur d'inventaire, l'auteur défriche hardiment le champ de la cyberstratégie et esquisse de multiples pistes de recherche permettant de s'approprier ce nouveau fait stratégique encore largement inexploré. Témoignage d'une véritable discipline stratégique qui apprend à se penser.

Le Vieil - p. 50

51 **L'usage de la force dans le cyberspace et le droit international**

LOÏC SIMONET

Comment qualifier une cyberattaque ? Ouvre-t-elle le droit à la légitime défense ? Comment résoudre la question de l'imputabilité de l'attaque surtout quand elle est infraétatique ? Autant de questions que se pose le juriste et que traite l'auteur.

57 Agir et réagir dans le cyberspace

Le Cadet - p. 62

VINCENT JOUBERT

Dernier territoire ouvert à la stratégie, le cyberspace s'intègre progressivement dans la stratégie militaire générale. Il reste à en calibrer les dimensions stratégiques défensives et offensives, juridiques et techniques et à en évaluer le potentiel dissuasif. C'est à cet effort analytique que participe l'auteur qui s'attache à cerner la capacité offensive qu'il recèle.

63 *Advanced Persistent Threats* : quelles réponses ?

SÉBASTIEN HÉON

Contrepartie des progrès informatiques, les vulnérabilités enkystées dans les systèmes sont autant de portes d'entrée pour des prédateurs. Détecter, circonscrire et réparer les dégâts causés par des intrusions malveillantes demande l'aide d'un tiers bienveillant et d'une méthodologie rigoureuse. Point de situation.

Repères - Opinions - Débats

71 Six enseignements stratégiques de l'opération *Unified Protector* de l'Otan en Libye

FLORENCE GAUB

L'opération de l'Otan principalement aérienne a été combinée avec les forces rebelles au sol. Plusieurs premiers enseignements peuvent en être tirés, sur le rôle de la puissance aérienne, la mise en œuvre d'un QG opérationnel, la connaissance du milieu, la communication stratégique ou la cohérence politico-militaire.

78 Mali : vive la Coloniale !

CLAUDE LE BORGNE

C'est une pérégrination historique et sociologique que propose l'auteur pour prendre la mesure des troubles actuels qui affectent le Sahel, sous la pression des revendications *Touareg* qui révèlent la sage inertie des équilibres qui ont structuré l'empire africain français et dévoile les premiers effets pervers de la transition libyenne.

83 Le dilemme syrien du *Hezbollah*

JEAN-LOUP SAMAAN

Le *Hezbollah* libanais est aujourd'hui fragilisé par l'ébranlement du régime de Damas qui en a constitué un appui constant, bien que prudent, et complémentaire du soutien fourni par l'Iran. Le difficile rééquilibrage en cours affecte la vie politique libanaise et compromet les chances du *Hezbollah* de survivre à la crise.

88 Le Printemps arabe à l'épreuve du salafisme

KHALIFA CHATER

L'auteur propose dans ce texte documenté une généalogie soignée du courant salafite qui est aujourd'hui l'un des plus actifs de la saison arabe que connaît la Méditerranée. Partant de l'exemple égyptien et de l'expérience tunisienne, il montre que ce courant domine aujourd'hui l'Islam politique et structure les différents scénarios d'avenir de la région nord-africaine.

93 À propos d'*Afghanistan*, guerre lointaine ?

RENÉ CAGNAT

Cette réflexion éclairée de l'auteur, expert militaire régional, nous porte le message fort d'un livre qui dénonce la dérive technique du combat d'infanterie et prône une autre façon de combattre au XXI^e siècle, plus soucieuse de guerre juste face à l'ami impitoyable qu'est l'adversaire d'aujourd'hui en Afghanistan que d'attrition d'un ennemi resté lointain.

96 **Stratégie maritime intégrale : une approche conceptuelle**

LARS WEDIN

C'est à une approche intégrale de la stratégie maritime qu'il faut procéder aujourd'hui pour coordonner les activités maritimes et les nécessités navales, penser la politique maritime intégrée de l'Union européenne et reconnaître à la mer son unité, sa globalité et sa centralité dans la mondialisation.

102 **Le New START Treaty : un traité nécessaire ou dépassé ?**

STEVEN EKOVIKOVICH

En contractant un nouveau traité de réduction des armes stratégiques, États-Unis et Fédération de Russie redonnent vie à un dialogue stratégique ancien. Mais il n'est pas sûr qu'ils en fassent la même lecture et qu'ils s'engagent réellement sur la même voie, notamment du fait de l'hypothèque antibalistique qui les oppose.

111 **Quel avenir pour les DRH d'armée ?**

GAËL KERRÉNEUR

La profonde transformation que connaît le ministère de la Défense bouleverse la gestion des ressources humaines militaires. Après les décrets de 2009 qui réorganisent la gouvernance du ministère autour du chef d'état-major des armées, les DRH d'armées, si elles s'effacent devant l'EMA/RH, restent garantes de l'efficacité opérationnelle des armées et gardent leur raison d'être.

117 **L'universalisme occidental : illusion antique ou succès planétaire ?**

NICOLAS TENZER

Cette réflexion inspirée sur l'universalisation de la planète et sur ses différents espaces de progression actuels, loin de reprendre la prétention occidentale à un avant-gardisme universel est une invitation à l'ouverture et à l'exemplarité individuelle et collective du monde développé.

Revues - Rapports

125 **Analyse stratégique** - La Chaire Castex de cyberstratégie

FRANÇOIS GÉRÉ

126 **CICDE** - Travaux de concept et de doctrine de cyberdéfense

SÉBASTIEN GOURTAY

128 **Parmi les livres** - Marins, explorateurs, roman maritime

EUGÈNE BERG

132 **Méditerranée** - Espaces maritimes et articulations transnationales

YVES HENOCQUE

135 **Russie** - La longue route de la Russie vers l'OMC

ALEXANDRE KAUFMANN

137 **Asie** - Trois théâtres chauds

DANIEL SCHAEFFER

Recensions

143 Henry Kissinger : *De la Chine*

Bernard Maréchal : *Le Grand jeu sino-américain - Essai sur le devenir du monde*

Irnerio Seminare : *Six études sur les équilibres internationaux*

Michel Bourgin : *Chroniques touarègues*

CYBERSTRATÉGIE

Supplément électronique diffusé en accès libre
www.defnat.com

Wikileaks ou le paradoxe de la transparence

STÉPHANE DOSSÉ

Cette réflexion sur le secret, sa relation aux libertés individuelles et collectives et à la protection de la sûreté des États éclaire l'ambiguïté de l'action de ceux qui ont lancé la dynamique de divulgation de *Wikileaks*.

De la disruption massive à la cyberguerre probable

CHARLES BWÉLÉ

À l'ère informationnelle, quelques lignes de code peuvent causer de sérieuses nuisances ou semer le chaos dans le monde réel. D'où la nécessité de réinventer nos approches parfois vieillissantes de la guerre et d'intégrer le domaine cybernétique dans le champ conflictuel comme un espace d'affrontement décisif.

Cyberstratégie à la Russe

YANNICK HARREL

C'est par les textes fondateurs d'une véritable réflexion sur la guerre informationnelle que l'on peut prendre la mesure de l'importance désormais décisive qu'accordent les autorités russes au cyberspace et à la stratégie informationnelle érigés en priorité de la Fédération de Russie.

L'espace extra-atmosphérique et le cyberspace : exploration d'une relation symbiotique

GUILHEM PENENT

Deux domaines récemment prospectés et interconnectés – l'espace extra-atmosphérique et le cyberspace – définissent un nouveau champ de forces, d'affrontements et d'occasions à saisir pour ceux qui y ont accès et savent en combiner les effets. Loin d'avoir la même consistance, ils sont désormais ouverts à la compétition et au conflit.

Le capital humain, enjeu national pour la sécurité du cyberspace

MARTIAL IMBERTI

C'est dans l'expertise humaine comme dans l'organisation globale qu'il faut aujourd'hui faire effort au moins autant que dans l'innovation technique et l'expérimentation pour relever le défi de sécurité que révèle le cyberspace comme espace de vulnérabilité et champ de friction voire d'affrontement.

La violence et le cyberspace

THIERRY RANDRETSA

Dans cette réflexion soignée sur la singularité des attaques informatiques vues au prisme du *jus ad bellum* et du *jus in bello*, l'auteur passe en revue les questions essentielles de la légitime défense, de la neutralisation et de la virtualité de l'action au vu de la violence exercée. Il y voit une mutation de la guerre.

L'être militaire à l'épreuve du cyber

BRUNO DEPARDON

La politique de défense voit son objet principal mis en cause par la dématérialisation et la déterritorialisation des pouvoirs. L'évidence « westphalienne » du militaire comme garant de la survie du pays et principal instrument de sa défense s'estompe. La révolution cybernétique affecte l'être militaire et l'oblige à se repenser dans son environnement numérique.



L'Armée de terre face à ses missions

Bertrand Ract Madoux

Général d'armée, chef d'état-major de l'Armée de terre.

Quelques mois passés à la tête de l'Armée de terre, auxquels s'ajoutent plusieurs années passées hors de ses rangs, me permettent aujourd'hui d'apprécier avec recul, et à leur juste valeur, la bonne image que cette dernière renvoie ainsi que la maturité professionnelle dont elle fait preuve dans chacun de ses engagements. Cette maturité s'est notamment forgée dans des opérations particulièrement dures au cours desquelles nombre de nos camarades ont versé leur sang dans l'accomplissement de leur devoir.

Je constate ainsi combien, entre 2008 et 2012, dans un contexte de lourdes réformes structurelles et fonctionnelles, elle a toujours su répondre aux attentes et remplir avec efficacité toutes les missions opérationnelles qui lui ont été assignées, que ce soit en métropole, outre-mer ou à l'étranger.

L'an dernier, elle a notamment dû mener, de manière quasiment simultanée, trois opérations de guerre, de nature différente, sur des théâtres distincts, en République de Côte d'Ivoire, en Afghanistan et en Libye. Malgré des conditions d'engagement délicates, l'efficacité opérationnelle de nos unités et le courage de nos hommes ont été reconnus de nos concitoyens, de nos dirigeants politiques mais également de nos alliés.

Je retiendrai donc la pertinence des choix faits par le passé, par mes prédécesseurs, en termes d'équipements, de doctrine, d'entraînement et de préparation opérationnelle. Ils ont montré toute leur adéquation au cours de ces opérations. La justesse de ces choix s'est notamment exprimée par l'engagement des matériels les plus modernes en opérations, à peine leur mise en service opérationnel déclarée, à l'image des véhicules blindés de combat d'infanterie (VBCI), des hélicoptères *Tigre* ou du système d'armes *Felin* pour les combattants débarqués. Nos soldats peuvent ainsi s'entraîner en garnison sur des matériels identiques à ceux sur lesquels ils seront amenés à servir en opérations ; les opérations

d'adaptation réactive permettant de prendre en compte, à la marge, les spécificités ou les exigences des théâtres d'opérations.

Cette efficacité remarquable est très certainement le fruit des profondes restructurations menées depuis 2008 qui ont fait de l'Armée de terre un outil de combat moderne, ramassé et cohérent, apte à répondre aux missions qui lui ont été fixées par le *Livre blanc sur la défense et la sécurité nationale* de 2008. Peu de pays au monde ont encore une Armée de terre capable de répondre à l'ensemble de l'éventail des opérations. La France en fait partie. Il s'agit là d'une expression concrète de son ambition.

Ce bilan très positif ne doit néanmoins masquer les difficultés de fonctionnement courant que vivent au quotidien nos régiments. Aux bouleversements apportés par la réforme du soutien et la création des bases de défense pour lesquels il faudra laisser du temps avant une appropriation optimale des nouveaux processus, s'ajoute un contexte de contraintes budgétaires qui exerce une pression croissante sur nos crédits de fonctionnement et d'entraînement. L'engouement du personnel de l'Armée de terre pour son métier, le sens du bien commun qu'il manifeste et ses facultés d'adaptation permettent heureusement d'aller résolument de l'avant et de se projeter dans un avenir paradoxalement toujours plus incertain.

À l'heure où s'opposent contraintes sur les finances publiques et incertitudes géopolitiques, l'Armée de terre doit, en effet, relever plusieurs défis nés de facteurs exogènes dont la conjugaison pourrait laisser penser que l'engagement de soldats au sol est moins utile voire moins légitime qu'auparavant.

Le premier de ces facteurs est, pour un pays comme la France, l'éloignement conjugué de la menace des combats aux frontières et des opérations extérieures, qui contribue à écarter l'idée de danger de l'esprit de nos concitoyens.

Le deuxième est le développement technologique qui peut parfois laisser croire que la guerre pourrait être menée et gagnée sans homme ou, tout du moins, sans homme au sol. Certaines analyses des opérations conduites en Libye sont, à ce titre, révélatrices, faisant fi des bataillons de soldats libyens des deux bords qui se sont affrontés pour le contrôle des villes et nœuds de communications, tout comme de l'action des hélicoptères agissant dans une manœuvre aéroterrestre.

Troisième facteur et non des moindres, la mort au combat de soldats et sa médiatisation peut désormais prendre un poids accru dans l'opinion publique et agir sur la détermination nationale. Ce facteur ne peut désormais être ignoré, y compris dans la conduite des opérations, malgré le risque d'inhibition qu'il peut faire peser sur la prise de décision. Nos adversaires d'aujourd'hui le savent et peuvent plus facilement en jouer du fait de la mondialisation médiatique.

Les contraintes sur les finances publiques des pays européens, notamment, viennent enfin fragiliser les besoins des armées engagées dans un indispensable

renouvellement de leurs matériels et parc de véhicules. Concernant l'Armée de terre, cet effort de long terme, commencé avec le char *Leclerc*, le *VBCI* et le *Tigre*, est ainsi appelé à se poursuivre dans le cadre du programme *Scorpion*. Celui-ci est destiné à fournir les équipements majeurs des groupements tactiques interarmes à partir de 2016 et remplacer des matériels vieillissants. Il verra notamment l'acquisition de nouveaux engins de la classe 20 tonnes, le véhicule blindé multi-rôle (le *VBMR*) pour remplacer les vénérables *VAB* et l'engin blindé de reconnaissance et de combat (*EBRC*) en lieu et place des *AMX 10RCR* et *ERC 90*. Ce besoin de modernité est à la hauteur des défis d'avenir d'autant que la coexistence de matières modernes et obsolètes mettrait à mal la cohérence de l'Armée de terre.

Or, contrairement à ce que Vigny pouvait penser en affirmant que « les armées et la guerre n'auront qu'un temps », il apparaît probablement que ce temps ne soit pas encore venu. L'avenir des actions militaires et donc celui des forces terrestres semble bien assuré dans la mesure où « c'est bien là où vit l'homme, que se déclenche la guerre et se gagne la paix ».

Un éventuel recours à la force armée, et en particulier de l'action terrestre, ne peut ni ne doit donc être éludé ou relever du tabou. Le monde est en pleine période d'incertitude géopolitique. À l'exception des pays européens, de nombreuses nations réarment. Non loin de la France, le pourtour méditerranéen traverse une période de turbulences dont nul ne sait comment il en sortira.

Dans ce contexte trouble, l'Armée de terre peut apporter, au sein des armées, une réponse crédible et adaptée. Sa principale caractéristique est, en effet, d'être un outil polyvalent et réversible, adapté à la fois à la complexité des milieux humains et des menaces. Elle tire sa force de sa cohérence et de sa capacité à agir dans un cadre interarmées en nombre et dans la durée. Ces aptitudes reposent sur un seul acteur, l'homme, valorisé par des systèmes d'armes de dernière génération. Son engagement est, et demeurera, indispensable pour apprécier les situations, graduer et maîtriser le niveau de violence, réagir aux évolutions de la situation, s'adapter à un milieu qui, s'il est peut-être plus accessible que les autres, n'en est pas moins complexe et exigeant, en raison, notamment, de son hétérogénéité et de l'imbrication quasi systématique avec les populations.

Apte à combattre lorsque cela est nécessaire, l'Armée de terre est aussi l'armée du retour à la normalité, en opérations extérieures comme sur le territoire national, en cas de besoin. L'engagement de 100 000 soldats des forces d'auto-défense japonaises après la catastrophe de Fukushima est un exemple qui mérite toute notre attention. Aujourd'hui ramassée sur ses seules forces de combat, l'Armée de terre va, cette année, franchir à la baisse ce seuil symbolique. Face à une catastrophe naturelle, qui plus est d'une ampleur comparable, nos concitoyens attendront légitimement que celle qui demeure l'armée du territoire intervienne à leur profit.

La capacité opérationnelle de l'Armée de terre repose donc et avant tout sur ses hommes dont l'action est rendue efficace par le recours aux équipements les plus modernes du moment. Ainsi, contrairement aux idées reçues, le métier de soldat n'est pas simple. Le service de matériels de dernière génération et la complexité croissante des opérations terrestres induisent un apprentissage initial conséquent puis un entretien complet, progressif et cohérent de savoir-faire techniques et tactiques en constante évolution. Cette exigence doit permettre de réduire au maximum les risques encourus en opérations.

*
**

Les différentes réformes conduites depuis le début des années 90, ont abouti à l'Armée de terre d'aujourd'hui, conforme aux décisions du *Livre blanc sur la défense et la sécurité nationale*. Ramassée et rationalisée, loin de l'image d'une armée de gros bataillons qu'elle a pu avoir du temps de la conscription, elle est un outil de combat efficace et cohérent, à la hauteur des ambitions de la Nation.

Il lui faut maintenant achever sa modernisation afin d'être capable de répondre aux combats de demain, des combats probablement plus durs et plus dispersés, ainsi qu'aux sollicitations et événements imprévus. Ce besoin de modernité et de cohérence est essentiel à la capacité opérationnelle future de l'Armée de terre. Mais je suis pleinement conscient que l'indispensable effort de redressement des finances publiques ne devrait certainement pas rendre facile la résolution de cette délicate équation.



La Chine, le nouveau « Péril jaune »

Pierre Conesa

Ancien directeur-adjoint de la Délégation aux affaires stratégiques, auteur de *La fabrication de l'ennemi ou comment tuer avec sa conscience pour soi* (Laffont 2011), préface de Michel Wievorcka.

L'Amérique entrant dans la campagne présidentielle, la Chine devient plus que jamais dans les discours des candidats aux primaires républicaines « l'ennemi », c'est-à-dire cet Autre, ce compétiteur potentiellement menaçant, commercialement, économiquement, financièrement, informatiquement et évidemment militairement. Le *New York Times* du 9 octobre 2010 dénombrait 19 Démocrates et 10 Républicains qui fondaient leur campagne locale en usant de « diabolisation culturelle et raciale » contre la Chine. Identifier une menace et prétendre la gérer est un élément essentiel du programme de tout candidat. Historiquement les voix dominantes ne sont pas venues du gouvernement mais des *think tanks* et des éditorialistes néoconservateurs : William Kristol dans son *Weekly Standard*, décrit la République populaire de Chine, la RPC, comme « d'une barbarité structurelle », rejoint en cela par Robert Kagan, cofondateur du désastreux « *Project for a New American Century* »⁽¹⁾ et de nombreux autres.

Qu'est-ce qui fait la spécificité de « l'ennemi chinois » ?

C'est certes le compétiteur le plus sérieux de la suprématie américaine⁽²⁾ mais est-ce pour autant une menace militaire ?

Evan B. Tracey, président du *Campaign Media Analysis Group*, qui analyse les publicités électorales, dit que la Chine est devenue le repoussoir comme l'était

(1) Le « *Project for a New American Century* » qui a donné naissance aux concepts stratégiques de l'équipe de G. W. Bush, annonçaient les voies et moyens d'empêcher un compétiteur à la puissance américaine d'apparaître.

(2) « *A near peer competitor* » disent les Anglo-Saxons.

le Japon dans les années 1980, à l'occasion de la crise de l'automobile, et le Mexique, lors de la signature du *NAFTA* ⁽³⁾. L'*Economic Policy Institute*, un autre *think tank* proche des Démocrates, évaluait, il y a quelques années, à 3 millions, le nombre d'emplois perdus depuis 2001 du fait des déficits commerciaux à l'égard de la Chine. « Nous avons vécu une décennie avec *Al-Qaïda*. Nous surveillons aujourd'hui la Chine ». Économiquement la nouvelle puissance économique chinoise est une réalité mais à échéance incertaine. Justin Lin, chef économiste de la Banque mondiale, lui donne la première place mondiale en 2030, le rapport de la Standard Chartered Bank de 2011 prévoyait 2020 et un rapport de l'OCDE de 2007 annonçait 2015. Beijing, premier détenteur de bons du Trésor américain, a critiqué les déficits publics (« l'addiction américaine à la dette ») et la politique fiscale laxiste, sans doute soucieuse de préserver ses avoirs. Paroles admissibles chez un économiste de *Wall Street* mais probablement pas venant de responsables communistes chinois. Acculés par la crise, les dirigeants occidentaux demandent instamment à la Chine de réévaluer sa monnaie et ainsi de réduire ses excédents commerciaux, ce à quoi Beijing répond que, devant créer environ 60 millions d'emplois dans les vingt prochaines années, les « bons vieux temps » de l'État-providence étaient finis et que donner du travail aux Chinois restait la priorité. On en arrive à oublier que la crise économique et financière est née à *Wall Street*.

Affrontement préventif face à une montée en puissance régulière ?

Le recours à la force, voire la guerre, avant que la puissance militaire ne tourne au désavantage des États-Unis, est entré progressivement dans le débat stratégique dans la décennie 1990 quand se formalise la pensée néoconservatrice. Paul Wolfowitz, en visite à Pékin en 2005, s'émouvait de la dépense militaire du pays qui avoisinait les 90 milliards de \$ quand le budget américain frisait les 700 milliards.

De fait, l'effort militaire chinois est resté plafonné à 2 % du PIB depuis vingt ans, alors que celui des États-Unis atteignait des pics à 4,7 %. Selon des calculs du Sipri, un *think tank* suédois réputé, il faudrait réévaluer en 2011 le budget de l'Armée populaire de Libération, l'APL, à 160 milliards de \$ au lieu des 120 officiellement déclarés, pour y inclure des dépenses de R&D militaires. Mais on est toujours dans des enveloppes 4,5 fois moindres que celles du Pentagone. La croissance du budget de défense suit la croissance économique chinoise (près de 12 % par an sur les deux dernières décennies). En l'espèce faut-il parler de croissance mécanique du budget militaire ou de volonté belliciste ? Les vieux habitués de la réflexion stratégique se rappellent sans doute l'époque des années 1970-1980 quand, impressionnés par la croissance soutenue de l'économie japonaise, on s'inquiétait de l'effort militaire de Tokyo qui construisait « un sous-marin par an » ou qu'on lui supposait des efforts secrets pour se doter de l'arme nucléaire.

(3) Pour *North American Free Trade Agreement*.

La mutation de l'armée chinoise est surtout qualitative. Les responsables militaires de Beijing ont révisé leur copie après la démonstration de force américaine lors de la guerre du Golfe. Ils ont alors avalé à doses accélérées les écrits d'Andrew Marshall et sa « Révolution dans les Affaires militaires ». C'est ainsi que dans ses rapports annuels publics, le Pentagone s'est inquiété de la montée en puissance de l'APL en insistant sur ses efforts en matière de *CAISR* ⁽⁴⁾. Les rapports américains ont vocation certaine à encourager l'effort de défense, c'est-à-dire à renforcer la thèse des experts, notamment républicains, qui ne cessent d'alerter le Congrès et l'opinion sur le fait que la Chine est, à long terme, le seul véritable ennemi stratégique des États-Unis.

En 2012, la RPC a critiqué la « Nouvelle stratégie de défense » du Pentagone, qui, selon elle, vise à l'isoler en Asie du Sud-Est et adopte une posture provocatrice et menaçante frisant au *Containment*. Le président Obama s'en défend mais faut-il s'étonner que le concept stratégique chinois soit qualifié par les Américains de *2A/AD* (*anti-access/area denial*), c'est-à-dire visant à interdire l'accès à une puissance militaire étrangère (manière indirecte de désigner les États-Unis) autour d'une « première chaîne d'îles ». Dans un monde multipolaire, quel gouvernement n'afficherait pas des intentions stratégiques identiques pour garantir la sécurité du pays ? Seuls les Occidentaux continuent à s'accorder une vertu de police planétaire, malgré l'Irak et l'Afghanistan.

Si « un ennemi s'attaque à vos intérêts nationaux, cela signifie que l'ennemi a déjà tiré le premier coup... donc l'armée doit tout faire pour dominer l'ennemi en frappant la première ». Cette doctrine de la guerre préventive n'est pas tirée des réflexions d'un néoconservateur américain mais est extraite d'un document de doctrine publié en 2005 par le journal chinois *Science de l'Art militaire*. La Chine cherche aussi à maintenir son accès aux ressources et aux marchés indispensables à son développement économique et ainsi à établir une présence et une influence régionales susceptibles « d'équilibrer et d'entrer en compétition avec d'autres puissances, dont les États-Unis, le Japon et l'Inde, dans des zones éloignées des frontières de la Chine », note le Pentagone.

Finalement la Chine mènerait la même diplomatie que les États-Unis. Sa flotte militaire doit être en mesure d'évacuer ceux de ses 5 millions de ressortissants qui se trouvent dans des zones en crise, comme elle l'a fait en Libye l'an dernier pour ses 35 000 expatriés. Ce n'est pas la France qui pourrait trouver à y redire. Accessoirement on remarquera qu'en 2012 l'effort d'équipement des forces de sécurité intérieure a dépassé celui des forces armées, démontrant que pour l'heure le Parti communiste est plus préoccupé par les menaces intérieures qu'extérieures ⁽⁵⁾.

(4) Pour *Command, Control, Communications, Computers, Intelligence* (Renseignement), *Surveillance and Reconnaissance*, comme toutes les armées modernes.

(5) Cf. *The Economist* 7-13 avril 2012, p. 28.

Péris jaune

N'était la différence d'époque, on croirait entendre la mythologie du « Péris jaune » si chère à nos grands-parents (stratèges ou pas). Jacques Decornoy ⁽⁶⁾ démontre que le Péris jaune est la continuité du mythe des Barbares « expression occidentale d'une peur de la décadence ». Forcée en pleine poussée coloniale européenne, l'expression de « Péris jaune » serait attribuée à Guillaume II lors de la tentative de « fédérer » les nations occidentales ayant des colonies en Asie. Le terme lancé après les deux guerres de l'Opium (1837-1842 puis 1857-1860) faites par la France et l'Angleterre pour ouvrir le marché chinois à la drogue produite par leurs colonies entre rapidement dans la culture populaire par divers ouvrages de romanciers, essayistes, militaires, géographes et diplomates. La métaphore entomologique de la « fourmilière » asiatique ou anthropologique insistant sur le caractère cérébral primaire, l'obéissance innée ou la cruauté des populations jaunes, se double de l'effroi face à la démographie chinoise. De temps en temps, le péril est décrit comme menaçant, de temps en temps comme peu crédible quand les Chinois se font battre par les Japonais : « On s'est aperçu dans ces derniers temps que les Chinois éprouvent une horreur insurmontable contre le service militaire » écrivait alors un commentateur d'un journal populaire français.

L'argument culturaliste apparaît aujourd'hui encore dans les analyses de l'ancien président de la Commission des affaires étrangères, de la défense et des forces armées du Sénat : « Il ne faut pas sous-estimer la valeur militaire des Chinois ». Le général de Gaulle aussi céda aux délices du « Péris jaune » dans le discours de Brazzaville en 1945 : « Voilà pourquoi nous allons former cette Communauté franco-africaine [...] parce que nul n'ignore qu'il y a de grands dangers [...] dans le monde, des menaces qui pèsent sur l'Afrique [...], particulièrement en Asie, de grandes masses humaines qui cherchent à s'étendre faute d'avoir avec elles des moyens suffisants pour vivre ».

On en retrouve aujourd'hui la version mise à jour dans les inquiétudes stratégiques françaises, tout à coup soucieuses de ne pas voir sur le continent africain, une autre puissance envisager les mêmes méthodes que celles de la Françafrique. La Chine misérable effrayait les colonisateurs par sa masse démographique (« 400 millions d'habitants, 30 millions d'hommes en armes » annonçait-on à la fin du XIX^e siècle – aujourd'hui 2,3 millions de soldats seulement pour 1 200 millions d'habitants) ; la Chine communiste du maoïsme devint la nouvelle menace après 1949 (alors qu'elle mena deux conflits contre d'autres pays communistes) et enfin la Chine moderne fondée par Deng Xiaoping, fait peur par sa croissance économique. Le schéma intellectuel est le même mais change de support.

(6) Cf. J. Decornoy : *Péris jaune, peur blanche* ; Grasset, 1970.

Quel rôle pour la Chine ?

La Chine joue-t-elle aujourd'hui un rôle stabilisateur ou déstabilisateur ? « Quand on parle aux officiels indiens, les relations sont présentées comme harmonieuses, aplanies. Officieusement, les Indiens ont peur des Chinois. Une confrontation entre les deux grands États n'est pas inenvisageable », met en garde M. de Rohan. « La Chine qui était autrefois bornée par ses frontières intervient un peu partout, notamment en Afrique. Elle passe à l'offensive dans la mer de Chine », annonce l'ancien Président. « L'affaire récente des chalutiers qui a conduit le Japon à réviser sa politique de défense démontre que la montée en puissance de l'Empire du milieu ne laisse pas indifférent », note plus prudemment Thierry de Montbrial, directeur général de l'Ifri dans *L'État du monde 2010*. La géopolitique chinoise inclut évidemment Taiwan mais aussi la mer de Chine du Sud. C'est là que les rivalités intra-asiatiques avec le Japon, le Vietnam, la Corée et les Philippines sont les plus sensibles. Ces questions peuvent se résoudre par recours à la justice internationale comme devraient l'être les différends naissants dans la zone arctique entre Canada, États-Unis, pays scandinaves et Russie. Les mises en garde contre les intentions chinoises seraient plus compréhensibles si elles n'émanaient pas de Washington qui vient à peine de quitter l'Irak.

La RPC est devenue le plus gros contributeur en hommes des 5 membres permanents du Conseil de sécurité pour les opérations onusiennes et a participé à une vingtaine d'opérations de maintien de la paix. Comme le faisait remarquer le général Yao Yunzhu, de l'Académie militaire : « On est critiqué si on fait moins et on est critiqué si on fait plus ; les pays occidentaux qui dominent l'ordre militaire international avec l'Otan et les accords de défense en Asie, devraient savoir ce qu'ils veulent ! ». Militairement l'Europe reste fascinée par les analyses américaines. Pourtant l'armée chinoise n'est pas sortie de ses frontières depuis les accrochages avec l'armée vietnamienne dans la désastreuse contre-offensive-défensive de 1979. Sa valeur opérationnelle est douteuse et son intention de se doter de 3 porte-avions suppose une longue période d'apprentissage que beaucoup de pays affichant les mêmes équipements n'ont jamais réussi à franchir. On ne peut en dire autant des armées des deux plus grandes démocraties, l'armée américaine embourbée en Irak et en Afghanistan, ni de celle de la République indienne qui a mené 6 guerres extérieures depuis l'Indépendance mais conserve à vie le titre de « pays de la non-violence ».

La Chine a une vision différente des solutions à apporter à la crise nucléaire iranienne et on peut raisonnablement penser qu'elle joue un rôle moins déstabilisateur que d'autres qui semblent envisager la guerre avec légèreté. On peut reprocher à Beijing de refuser le mandat qui permettrait une action onusienne en Syrie, certes ! Mais peut-être pourrait-on dans le même débat onusien, rappeler les innombrables mandats demandant le retrait des territoires occupés depuis 57 ans par Israël et systématiquement bloqués par Washington. La Chine est un pays dictatorial, certes ! Impérialiste ? Pas plus que d'autres, y compris des grandes

démocraties. En fin de compte, on reproche à Beijing de faire la politique des néo-conservateurs américains.

En tant qu'Européens, doit-on comme ces derniers, considérer l'expansion chinoise comme un danger ou au contraire aider Pékin à s'intégrer dans le concert international ? Quand un bateau de guerre chinois apparaît dans le golfe Arabo-Persique pour « sécuriser les voies d'approvisionnement pétrolières » comme nous le faisons nous-mêmes, faut-il y voir une menace ou une contribution à la sécurité internationale ? Les instabilités stratégiques naissent dans les périodes de changement où une nouvelle puissance cherche sa place dans des règles internationales à réviser. La Chine possède aussi avec *Global Times*, son propre *Fox News*, le groupe de médias de Rupert Murdoch qui a préparé à l'invasion de l'Irak et qui diffuse à jets soutenus du « Péril jaune ». La stupide démarche guerrière possède ses supports des deux côtés.

Éviter l'affrontement suppose de tenter de comprendre la position de l'Autre, pas de la diaboliser. On attend de l'Europe qu'elle contribue à aider la Chine à prendre sa place plutôt qu'à répéter le discours de « l'ennemi chinois ». C'est ce qu'a tenté de faire Jean-Pierre Raffarin, le « Monsieur Chine » du précédent gouvernement français.



Enjeux et perspectives de la sécurité maritime mondiale

Patrick Boissier

| Président-directeur général de DCNS.

La maritimisation du monde

La mondialisation se traduit par une interdépendance de plus en plus étroite entre pôles de peuplement et zones d'exploitation ou de transformation des ressources nécessaires à la vie humaine. Autrefois, ces zones étaient proches et concentrées autour de populations dont l'activité couvrait globalement les besoins. La raréfaction de certaines ressources et la croissance considérable de la consommation, auxquelles il faut ajouter le très faible coût du transport maritime ainsi que d'importants différentiels de coûts de main-d'œuvre, ont modifié l'équilibre autarcique ancien.

Dans cette évolution, la mer a pris une importance de plus en plus grande. D'abord pour la facilité qu'offrent les navires, vecteurs privilégiés des échanges de marchandises depuis des temps immémoriaux ⁽¹⁾. Ensuite et par conséquence, parce que les zones de production se sont installées préférentiellement sur des voies navigables ou à proximité du littoral maritime, où se concentre désormais la majorité de la population mondiale.

Mais cette population augmente encore de façon sensible, alors que les ressources terrestres s'épuisent ou approchent de leurs limites en termes de développement durable (minerais, énergie, agriculture). D'autres matières premières et sources d'énergie sont indispensables pour nourrir la population et subvenir à ses besoins. Où les trouver, sinon en mer ?

On mesure déjà concrètement l'extraordinaire réservoir de ressources que représente l'océan quand on observe le développement actuel des activités basées

(1) Les routes maritimes ne furent pas que commerciales. Elles permirent la diffusion des religions, des écrits, des cultures et des modèles politiques.

au large, *offshore*. Pétrole, gaz, énergie éolienne et aquaculture aujourd'hui ; énergie hydrolienne, minerais, terres rares et médicaments demain ; énergie thermique et biomasse pour alimenter la population en protéines après-demain. Sans parler du formidable champ d'exploration maritime qui reste à investir puisque nous n'avons probablement pas découvert plus de 10 % des espèces animales et végétales contenues dans les océans dont les fonds nous sont par ailleurs largement inconnus.

Dans cette quête de ressources vitales en mer les pays émergents ne sont pas les derniers à développer activement des stratégies maritimes très dynamiques pour ne pas dire offensives. Rien de fortuit dans ces démarches parfaitement rationnelles de leur point de vue et qui tendent à leur assurer le contrôle des ressources dont ils estiment avoir besoin. Cela couvre aussi bien les zones d'exploitation potentielle *offshore* que la sécurisation des routes maritimes jugées vitales pour leur développement.

La maritimisation du monde est en route. Elle se caractérise donc par un ensemble de réseaux qui relient entre eux les points nodaux constitués par les différentes zones de peuplement, d'exploitation et de transformation des ressources. Assez logiquement, l'essentiel des transports de produits de consommation dessert les zones de forte population, notamment sur la plus importante des routes maritimes, celle qui relie l'Europe à l'Extrême-Orient. Mais on voit émerger de nouvelles voies pour alimenter les pays en développement (Brésil, Afrique du Sud, Inde...), sans oublier celles dédiées aux minerais, au pétrole et au gaz. Sous ces routes de surface, au fond des mers, sont déployés de gigantesques réseaux de fibres optiques par où passe la quasi-totalité des communications mondiales.

Les vulnérabilités induites

Indissociable de la mondialisation, la maritimisation n'est donc pas un phénomène vraiment nouveau. Mais c'est son ampleur qui frappe et son développement spectaculaire risque d'engendrer un certain nombre de risques dont il faut bien prendre conscience.

La course croissante aux ressources maritimes va nécessairement susciter des compétitions et donc des tensions de plus en plus vives, notamment là où le découpage des zones économiques exclusives fait l'objet de contestations (mer de Chine du Sud et Arctique, par exemple). Par ailleurs, le statut actuel de la haute mer – *Res Nullius* – établi par les Européens à l'époque des grandes découvertes ne couvre en fait que la navigation. Il faudra bien définir des règles internationales d'exploitation durable pour l'énorme réservoir des ressources hauturières, y compris les fonds marins, véritable *Res Communis* de l'humanité.

De plus en plus denses, les routes maritimes elles-mêmes sont des lieux de tensions, singulièrement dans les détroits et passages resserrés ainsi qu'aux abords

des points nodaux que constituent les zones portuaires mais aussi dans les eaux internationales comme en témoigne une piraterie florissante en océan Indien et sur les côtes africaines.

Depuis le début du millénaire, le Pacifique Nord, l'océan Indien et dans une moindre mesure l'Atlantique Sud supplantent l'Atlantique Nord en termes de trafic maritime. Outre les routes maritimes traditionnelles – toujours très actives – de nouvelles voies se développent (notamment au Sud) pour transporter soit des produits finis par conteneurs, soit des matières premières entre la Chine, l'Inde, l'Indonésie, l'Australie, le Brésil, l'Afrique, la Russie. Dans peu de temps, le canal de Panama aura doublé de capacité, ouvrant le passage aux porte-conteneurs de 12 000 EVP, contre 5 000 aujourd'hui.

Si le réchauffement climatique se confirme, l'Arctique pourrait s'ouvrir à la navigation avec des conséquences significatives à moyenne échéance : transport possible de matières premières jusque-là inexploitées (Sibérie, Alaska, etc.), routes maritimes nouvelles et plus courtes entre l'Extrême-Orient, l'Europe et l'Amérique du Nord.

La mer territorialisée

Outre la croissance du trafic commercial et le développement du réseau des voies maritimes qui resteront le vecteur privilégié de la mondialisation avec 90 % du tonnage transporté, il faut aussi considérer la création puis l'extension inexorable de zones d'exploitation des ressources de la mer, de plus en plus denses et étendues.

La délimitation des zones côtières, littorales et économiques exclusives, les ZEE, a commencé à marquer la territorialisation des mers : zones arrimées aux pays riverains, avec tout ce que cela comporte de gestion d'interfaces et de sources de conflits. L'exploitation à venir de ressources maritimes considérables et encore bien mal connues (énergie, matières premières ⁽²⁾, biologie) va très probablement accentuer cette tendance qui tend à reporter en mer le concept de frontière terrestre.

On se plaît à répéter que la France dispose de la deuxième zone maritime mondiale, avec une surface totale de près de 11 millions de kilomètres carrés. Pour l'instant, ce capital – ou plutôt cet espace de respiration – paraît peu attractif économiquement ; on ne sait pas encore le caractériser ni *a fortiori* le valoriser. Demain cependant, lorsque les zones côtières surexploitées seront devenues insuffisantes, on se rendra compte de l'importance première de cet immense réservoir de ressources vierges en plein océan, notamment dans le Pacifique Sud et l'océan Indien.

(2) Outre le pétrole et le gaz, des mines de diamant sont déjà exploitées en mer au large de l'Afrique du Sud.

De fait, les frontières maritimes de la France ne se situent pas sur le littoral métropolitain ni même à la limite des eaux territoriales (12 milles des côtes). Au travers des mers et océans, la France est d'ailleurs directement riveraine de la majorité des pays du monde. Si l'on veut bien les considérer de façon dynamique comme les limites raisonnables de l'endroit – ou du moment – à partir duquel on estime qu'une menace éventuelle ne peut plus être contrée *a priori*, les vraies « frontières » sont en réalité bien loin de nos côtes et situées principalement dans les ports d'embarquement des passagers ou de chargement des marchandises. Pour en donner une illustration concrète, les Américains sont en train de mettre en place un processus leur permettant le cas échéant d'interdire *in situ* en Chine ou ailleurs, l'embarquement d'une marchandise à destination d'un port américain. Suivre à la trace les marchandises et les hommes « de bout en bout », voilà l'objectif poursuivi. Cela étant, on en est encore loin, même pour les trafics « licites », et en particulier en pleine mer.

Aujourd'hui encore, savoir ce qui se passe sur l'eau est un vrai défi. Une « tenue de situation surface » fiable est loin d'être acquise *a priori*, même dans une zone limitée. Et une fois cette situation générale établie, encore faut-il en extraire l'information utile en l'occurrence, c'est-à-dire celle qui concerne des situations considérées comme illicites ou anormales, selon des critères à définir. Après avoir identifié les situations anormales, il faut enfin pouvoir intervenir pour y remédier. Cela demande naturellement des moyens *ad hoc* maritimes, aériens ou terrestres (ports...) mais aussi tout un arsenal de règles juridiques adaptées compte tenu d'un contexte international et transfrontalier, à la fois sous juridiction des États (autorités du pavillon et États côtiers) et international, en haute mer avec un régime juridique bien particulier.

Une tenue de situation maritime exhaustive et fiable, une capacité de tri, d'identification et de suivi des menaces suivant des critères de classification fixés par les responsables opérationnels, des moyens d'intervention pertinents et adaptés à toutes les menaces présentes et à venir, telle est l'ampleur du défi. Grâce aux compétences uniques acquises dans le domaine militaire, voilà ce que l'industrie navale française est capable de proposer, globalement, pour répondre aux défis actuels et futurs de la maîtrise des espaces maritimes.

La puissance maritime pour protéger la planète bleue

Diversification des routes maritimes, forte augmentation des tonnages transportés, extension des zones d'exploitation des ressources en mer, développement de la navigation de plaisance et de croisière : le monde qui se dessine devant nos yeux est de plus en plus bleu marine.

La puissance maritime reste au cœur de ces débats, présents et à venir. Sans moyen de surveillance et de contrôle des espaces maritimes, sans bâtiment de guerre

et navire de surveillance de l'État, pas de liberté de circulation, pas d'exploitation contrôlée et responsable des ressources de la mer, pas d'activité de loisirs ou encore scientifique. L'exemple de la piraterie – endémique et largement renaissante – montre bien les limites du concept de *Res Nullius* lorsque les moyens de surveillance et d'action sont réduits.

Des dispositifs étatiques de contrôle des activités en mer sont en train de se mettre en place, *via* des réseaux de senseurs corrélés à des bases de données et pilotés par des systèmes de gestion des informations. Mais les océans sont immenses et on ne peut imaginer maîtriser de tels espaces uniquement à distance. Les radars et les caméras de surveillance n'ont jamais rendu inutiles les gendarmes et les policiers.

Devant la menace de la piraterie que les marines de guerre peinent à contenir en raison du faible nombre de leurs plates-formes rapporté à l'immensité des océans et à l'intensité croissante du trafic maritime, certains armateurs privés renouent d'ailleurs avec les pratiques anciennes et dotent leurs navires de moyens de se défendre contre les attaques, avec toutes les dérives potentielles de tels choix.

Les pays émergents ont tous bien compris l'importance d'une marine puissante pour défendre leurs intérêts. À l'heure où les Européens réduisent la toile et peinent à définir une politique maritime ambitieuse, ces pays et ceux qui les entourent engagent d'importants programmes d'extension ou de renouvellement de leurs moyens maritimes. Conscients des ressources que recèle l'océan qui borde leurs rivages, certains pratiquent des stratégies d'intimidation – voire de déni d'accès – afin de se tailler la part du lion dans la répartition de richesses dont la « propriété » est encore incertaine.

Mais la haute mer est aussi l'espace privilégié de manœuvre des forces étatiques aéromaritimes et sous-marines, y compris nucléaires : celles des puissances navales historiques dont bien évidemment la France mais aussi, et de plus en plus, celles des marines des grands pays émergents dont les ambitions ne se limitent manifestement pas à patrouiller dans leurs zones économiques exclusives.

*

**

Le siècle qui s'ouvre est celui de l'océan, bien commun de l'humanité, réservoir amniotique de notre planète terrestre. Espérons que les États, au sein de l'ONU, trouveront les voies originales et pertinentes pour définir les règles de gestion durable de ce patrimoine immense, que les marines militaires auront pour mission de faire respecter.

De formidables possibilités de développement en mer s'ouvrent à nous ; c'est une chance unique à saisir car nous avons toutes les compétences pour relever ces défis à la fois techniques, économiques et sécuritaires avec nos partenaires, et notamment les Européens.

IL Y A 50 ANS

COLLECTION

Publication mensuelle 18^e Année - Juin 1962

REVUE DE DÉFENSE NATIONALE

LES GRANDS PROBLÈMES
NATIONAUX ET INTERNATIONAUX

militaires, économiques, politiques, scientifiques

30 MAI 1962

DATE D'ARRIVÉE 7 MAI 1962

Pierre M. GALLOIS	Deux budgets militaires, une politique de sécurité qui s'accommode du « déséquilibre de la terreur ».....	937
Gouverneur Paul MASSON	Décolonisation et sous-développement ..	954
J.N.	Les relations sino-soviétiques de 1956 à 1961	970
Colonel du LATTAY	La défense civile aux Etats-Unis	988
Pierre RONDOT	La crise syrienne, sa genèse, ses circonstances, son bilan (Déc. 1961 - Avril 1962).	1000
Suzanne LABIN	Le complexe de Mars-Maginot du monde libre	1011
Chef d'Escadron DELBREIL	L'homme de l'espace	1020
René VALLET	Physionomie de l'économie chinoise ...	1041
Jacques VERNANT	Politique et Diplomatie : La France et les conversations américano-soviétiques.....	1050
Paul COULBOIS	Actualité économique : La fin d'un « miracle »	1055
A TRAVERS LES REVUES	Nos forces armées d'aujourd'hui et de demain (Grande-Bretagne).....	1063

CHRONIQUES

Claude VALETTE : O.T.A.N. — Colonel E.J. BAUDE : Militaire. —	
Lieutenant-Colonel LEPEU : Aéronautique. — André REUSSNER : Maritime. — J. DESMARESCAUX : Outre-Mer.....	1079
BIBLIOGRAPHIE FRANCAISE ET ÉTRANGÈRE	1105

SERVICE DOCUMENTATION

1, PLACE JOFFRE PARIS (VII^e) LE NUMÉRO : 2 NF



■ **Cyberstratégie**

RDN

La cyberdéfense

Jean-Marie Bockel | Sénateur du Haut-Rhin, ancien ministre.

À la fin de l'année 2010, notre pays a été victime d'une vaste attaque informatique visant le ministère de l'Économie et des Finances, pendant la préparation de la présidence française du G8 et du G20. Cette attaque de grande ampleur, réalisée grâce à un « Cheval de Troie », a illustré une nouvelle fois une menace mal connue en Europe et singulièrement en France, mais croissante : les atteintes portées à la sécurité des systèmes d'information susceptibles de mettre en cause la défense et la sécurité nationales. Elle a mis en évidence l'importance des moyens à déployer pour se protéger de cette menace, ce que l'on désigne habituellement sous le terme de « cyberdéfense ».

Dès 2008, la Commission des affaires étrangères, de la défense et des forces armées du Sénat avait chargé l'un de ses membres, M. Roger Romani, d'étudier les enjeux liés à la sécurité des systèmes d'information. Dans son rapport d'information ⁽¹⁾ mon collègue dressait le constat que la France n'était ni bien préparée, ni bien organisée face à cette menace.

(1) « Cyberdéfense : un nouvel enjeu de sécurité nationale », rapport d'information présenté par M. Roger Romani au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat, n° 449 (2007-2008), publié le 8 juillet 2008.

Depuis quatre ans, les choses ont beaucoup évolué. Si cette menace a été identifiée par le *Livre blanc sur la défense et la sécurité nationale* de 2008, elle s'est toutefois considérablement accrue avec la multiplication du nombre d'attaques informatiques visant les États, les institutions ou les entreprises. C'est la raison pour laquelle la Commission des affaires étrangères et de la défense du Sénat a souhaité faire à nouveau le point sur ce dossier et m'a désigné comme son rapporteur sur la cyberdéfense, en octobre dernier. À l'issue d'auditions et de déplacements, notamment pour étudier les systèmes mis en place par nos principaux partenaires européens, un nouveau rapport d'information sur la cyberdéfense va être publié.

Que faut-il entendre par « cyberdéfense » ?

On parle souvent indistinctement de « cybercriminalité », de « cybermenaces », de « cyberattaques » ou de « cyberguerres ». Il faut bien comprendre que les méthodes utilisées à des fins de fraude ou d'escroquerie sur *Internet* peuvent l'être aussi, à une échelle plus vaste, contre la sécurité et les intérêts essentiels du pays. C'est le cas

avec la pénétration de réseaux en vue d'accéder à des informations sensibles ou avec des attaques visant à perturber ou à détruire des sites largement utilisés dans la vie courante, voire même des systèmes liés à la défense ou au fonctionnement d'infrastructures vitales, comme l'énergie, les transports ou la santé par exemple.

Dans mon esprit, la cyberdéfense est une notion complémentaire de la cybersécurité. La cyberdéfense recouvre la politique mise en place par l'État pour protéger activement des réseaux et des systèmes d'information essentiels à la vie et à la souveraineté du pays, et donc les informations qu'ils contiennent et les systèmes qui y sont connectés.

Une menace diffuse de plus en plus précise

Depuis les attaques informatiques massives qui ont frappé l'Estonie en 2007, il ne se passe pratiquement pas une semaine sans que l'on signale, quelque part dans le monde, des attaques ciblées contre les réseaux de gouvernements ou de grands organismes publics ou privés. Ces attaques peuvent être menées par des pirates informatiques, des groupes d'activistes, des organisations criminelles mais aussi par des entreprises concurrentes, voire par d'autres États. Les soupçons se portent souvent vers la Chine ou la Russie, même s'il est difficile d'identifier précisément les auteurs de ces attaques.

On peut donc s'interroger sur la nature de cette menace. Peut-on véritablement parler de « cyberguerre » ? Peut-on imaginer que des conflits se joueront sur des cyberattaques, qui se substitueraient aux modes d'action militaires traditionnels ? C'est sans doute une hypothèse extrême. Il est acquis en revanche que l'on ne peut guère concevoir désormais de conflit militaire sans qu'il s'accompagne d'attaques sur les systèmes d'information. C'est par exemple ce qui s'est passé en Géorgie en août 2008. Toutes les armées modernes ont commencé à intégrer ce facteur. On peut aussi penser que nous serons de plus en plus confrontés à des agressions se situant dans une « zone grise » intermédiaire, à des fins de chantage ou de représailles. Jusqu'à présent, ce type d'attaques n'a produit que des nuisances assez limitées. Mais, à mon sens, il ne faut guère se faire d'illusion, les vulnérabilités sont réelles et les savoir-faire se développent. On ne peut pas éviter de telles attaques. Mais on peut en limiter les effets en renforçant les mesures de protection et en prévoyant comment gérer la crise le temps du rétablissement des systèmes.

Une menace désormais prise en compte ailleurs

Il est frappant de constater que la cyberdéfense est désormais prise en compte par nos principaux partenaires et qu'elle commence à s'affirmer au sein des instances internationales, à l'image de l'Otan ou de l'Union européenne.

Aux États-Unis, le président Barack Obama s'est fortement engagé sur le sujet et a qualifié la cybersécurité de priorité stratégique. Il existe plusieurs organismes, au sein du Pentagone et du département d'État chargé de la sécurité nationale, qui interviennent dans ce domaine, comme l'Agence de sécurité nationale (*NSA*) ou encore le *Cybercommand*, inauguré en 2010 et qui est chargé plus particulièrement de protéger les réseaux militaires américains. De 2010 à 2015, le gouvernement américain devrait consacrer 50 milliards de dollars à la cyberdéfense et plusieurs dizaines de milliers d'agents travaillent sur ce sujet.

Au Royaume-Uni, le gouvernement vient d'adopter, en novembre dernier, une nouvelle stratégie en matière de sécurité des systèmes d'information. Le principal organisme chargé de la cybersécurité est le *Communications and Electronic Security Group (CESG)*, antenne du *Government Communications Headquarters*. Ce *GCHQ* compte environ 5 500 agents, dont environ 700 s'occupent des questions liées à la cyberdéfense. Malgré la forte réduction des dépenses publiques, le Premier ministre David Cameron a annoncé en 2010 un effort supplémentaire de 650 millions de livres sur les quatre prochaines années pour la cyberdéfense, soit environ 750 millions d'euros.

En Allemagne, le gouvernement fédéral a élaboré en février 2011 une stratégie en matière de cybersécurité. La coordination en incombe au ministre fédéral de l'Intérieur, auquel est rattaché l'office fédéral de sécurité des systèmes d'information (*BSI*), situé à Bonn, qui dispose d'un budget annuel de 80 millions d'euros et de plus de 500 agents.

Les cyberattaques sont désormais une menace prise en compte dans le nouveau concept stratégique de l'Alliance atlantique, adopté lors du Sommet de Lisbonne en novembre 2010. L'Otan s'est dotée en juin 2011 d'une politique et d'un concept en matière de cyberdéfense. Une autorité de gestion de la cyberdéfense ainsi qu'un centre d'excellence sur la cyberdéfense ont été créés. Pour autant, l'Otan n'est pas complètement armée face à cette menace. Ainsi, la principale unité informatique de l'Alliance n'est toujours pas opérationnelle 24 heures sur 24, 7 jours sur 7 et elle n'assure pas encore la sécurité de tous les réseaux de l'Otan. Plus généralement, l'Alliance doit encore déterminer quelle attitude adopter pour répondre à des cyberattaques lancées contre l'une de ses nations. Peut-on invoquer l'article 5 du Traité de Washington en cas de cyberattaque ? Les mesures de rétorsion doivent-elles se limiter à des moyens cybernétiques ou bien peut-on également envisager des frappes militaires conventionnelles ? Il n'y a pas encore de réponses claires à ces questions.

L'Union européenne a aussi un grand rôle à jouer car une grande partie des règles qui régissent les réseaux de communications électroniques relève de sa compétence. Elle peut donc agir pour l'harmonisation de certaines dispositions techniques au niveau européen qui sont importantes du point de vue de la cyberdéfense. Toutefois, la Commission européenne et de nombreux

pays européens ne semblent pas encore avoir pris la mesure des risques et des enjeux liés à la cyberdéfense.

La France a commencé à combler son retard

Le constat que M. Roger Romani avait dressé dans son rapport il y a quatre ans était assez brutal : face à cette menace réelle et croissante, la France n'était ni bien préparée, ni bien organisée. Il serait injuste de dire que rien n'avait été fait. Je pense au réseau *Intranet* sécurisé interministériel pour la synergie gouvernementale (ISIS) pour l'information classée « confidentiel défense ». Néanmoins, les lacunes restaient criantes : dispersion des différents acteurs et des moyens ; insuffisance des moyens humains ; absence d'une capacité centralisée de surveillance des réseaux de l'État et de détection des attaques informatiques. En d'autres termes, il paraissait absolument indispensable d'accélérer la prise de conscience des autorités politiques, de clarifier les responsabilités au sein de l'État et de renforcer résolument les moyens techniques et humains nécessaires à une vraie politique de cyberdéfense.

Le *Livre blanc* de 2008 a identifié ce besoin et donné une réelle impulsion à cette politique. En matière d'organisation, il a permis à cette politique d'être clairement identifiée avec la création, en juillet 2009, de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dirigée par M. Patrick Pailloux et rattachée directement au Secrétaire général de la défense et de la sécurité nationale, ce qui lui confère une autorité interministérielle. Le 15 février 2011, l'ANSSI a rendu publique la stratégie de la France en matière de cyberdéfense. Par un décret du 11 février 2011, il a également été fait de l'ANSSI l'autorité nationale de défense des systèmes d'information.

La France dispose, avec cette stratégie et avec l'ANSSI, d'outils importants pour la cyberdéfense. Pour autant, beaucoup reste à faire dans ce domaine. Ainsi, avec des effectifs qui devraient être de 280 personnes et un budget de l'ordre de 90 millions d'euros fin 2012, l'ANSSI est encore très loin des services similaires de l'Allemagne ou du Royaume-Uni, qui comptent entre 500 et 700 personnes. Pour accroître sa capacité d'intervention et de soutien, il a d'ailleurs été décidé, en mai 2011, d'accélérer l'augmentation des effectifs et des moyens de l'ANSSI, afin de porter ses effectifs à 360 d'ici 2013, ce dont je me félicite.

De plus, si les armées et le ministère de la Défense ont pris des mesures, les autres ministères ou opérateurs d'infrastructures vitales restent différemment sensibilisés à cette menace. Quel serait aujourd'hui le moyen le plus simple de provoquer une perturbation majeure de notre pays par le biais d'une attaque informatique ? Un moyen serait de s'en prendre au système bancaire ou à la distribution d'énergie. L'exemple du virus *Stuxnet*, qui a endommagé en 2009 les centrifugeuses de la centrale d'enrichissement de l'uranium de Natanz en Iran, montre que cela n'est pas une hypothèse d'école.

Quelles perspectives ?

Premièrement, il apparaît que nous ne sommes encore qu'au démarrage de la mise en place d'une véritable politique de cyberdéfense, tant au niveau national, que sur le plan de la coopération internationale. Il ne s'agit pas de prétendre à une protection absolue. Ce serait assez illusoire. Le propre des attaques informatiques est d'exploiter des failles, de se porter là où les parades n'ont pas encore été mises en place. Mais on peut renforcer la sécurité des réseaux et des infrastructures les plus sensibles, et améliorer leur résilience.

Deuxièmement, même si la cyberdéfense demeure avant tout une responsabilité nationale car elle concerne directement notre souveraineté, face à une menace qui s'affranchit des frontières, la coopération internationale sera déterminante. Elle existe, d'ores et déjà, entre les cellules gouvernementales spécialisées ou de manière bilatérale, notamment avec nos partenaires britanniques ou allemands. Elle arrive à l'ordre du jour d'enceintes internationales comme l'Otan ou l'Union européenne, qui pourraient s'impliquer plus activement, par exemple pour imposer un certain nombre de normes de sécurité aux opérateurs de réseaux. Deux conceptions s'opposent toutefois au niveau international : celle des pays occidentaux, qui veulent préserver l'espace de liberté que représente l'*Internet*, et celle des pays comme la Russie ou la Chine inquiets du rôle croissant des réseaux sociaux à l'image du Printemps arabe, et qui souhaitent renforcer le contrôle non seulement sur les systèmes mais aussi sur le contenu même des communications.

Troisièmement, il me semble que beaucoup reste à faire pour sensibiliser le monde de l'entreprise. Assurer la sécurité des systèmes d'information des entreprises n'est pas seulement un enjeu technique. C'est aussi un enjeu économique, puisqu'il s'agit de protéger la chaîne de valeur, notre savoir-faire technologique dans la véritable guerre économique que nous connaissons aujourd'hui, voire un enjeu politique, lorsque les intérêts de la nation sont en jeu. Or, avec l'espionnage informatique, notre pays, comme les autres pays occidentaux, est aujourd'hui menacé par un « pillage » systématique de son patrimoine diplomatique, culturel et économique.

L'État a aussi un rôle important à jouer pour soutenir le tissu industriel, et notamment les PME, qui développent en France des produits de sécurité informatique, pour ne pas dépendre uniquement de produits américains ou asiatiques. Se pose aussi la question des ressources humaines. Il existe aujourd'hui en France peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les entreprises ont du mal à en recruter. Nous devrions mettre l'accent sur la formation et développer les liens avec les universités et les centres de recherche.

Enfin, il faut nous poser la question délicate des capacités offensives. Pour ma part, je considère qu'on ne peut pas se défendre si l'on ne connaît pas les modes d'attaque et si l'on ne dispose pas d'une certaine capacité de

dissuasion. La lutte informatique offensive est prévue par le *Livre blanc* et la loi de programmation militaire. Mais toutes ses implications ne sont pas aujourd'hui clarifiées. Comment savoir si une attaque se prépare ou est en cours ? Comment établir l'identité des agresseurs ou la responsabilité d'un État ? Quelle doctrine d'emploi adopter ? Il faudra que nos experts trouvent des réponses à ces questions.

En définitive, compte tenu de la place croissante des systèmes d'information et d'*Internet* dans le fonctionnement de nos sociétés, je suis convaincu que notre défense et notre sécurité se joueront aussi sur les réseaux informatiques dans les années futures.

Le cyberspace : définitions, représentations

Daniel Ventre

Ingénieur au CNRS (Centre national de la recherche scientifique) et chercheur au CESDIP (Centre de recherches sociologiques du droit et des institutions pénales).

À l'heure où la cyberdéfense s'inscrit résolument comme un axe majeur des politiques de défense des nations industrialisées, où les cyberattaques sont souvent placées au rang des menaces les plus immédiates, le cyberspace, considéré par les États-Unis comme la 5^e dimension du combat et comme « un actif national stratégique »⁽¹⁾, reste paradoxalement assez mal défini.

(1) Le président Barack Obama, 2009, utilise l'expression « *National Strategic Asset* ».

Or tout espace – pour autant que le cyberspace en soit un – en raison de sa nature, de sa typographie, de sa géographie et surtout de la perception que l'on en a, conditionne l'action qui peut y être menée, les acteurs (compétences, profils, identités) qui doivent y être mobilisés, ainsi que les choix stratégiques, tactiques et politiques afférents à son utilisation.

Dans la réflexion qui suit, nous revenons dans un premier temps sur les principales caractéristiques des différentes définitions qui ont été formulées jusqu'alors⁽²⁾, puis proposons notre propre modèle construit autour de trois traits qui nous paraissent propres à définir le cyberspace : sa relation à l'espace informationnel, sa transversalité et sa structure en trois couches⁽³⁾.

(2) Une analyse bien plus détaillée du concept de « cyberspace » est proposée dans *Cyberspace et acteurs du cyberconflit*, Daniel Ventre, 2011, Éditions Hermès Lavoisier.

(3) Cette approche a été présentée lors de diverses conférences au cours de l'année 2011 et décrite dans *Cyber Conflict : Competing National Perspectives*, Daniel Ventre (Édit.), avril 2012, Éditions Wiley-ISTE.

Caractéristiques des définitions et représentations du cyberspace

La littérature (romans, nouvelles, science-fiction, *thrillers*, *cyberpunk*) mais aussi l'image (jeu vidéo, science, cinéma, cartographie) et bien sûr le discours militaire et politique, sont autant de sources de définitions et représentations du cyberspace.

De manière intuitive nous pourrions tout d'abord essayer de définir le cyberspace par référence à tout ce qu'il peut contenir : des puces électroniques, des ordinateurs, des infrastructures de communication, des satellites, des téléphones portables, des systèmes industriels informatisés, les données qui transitent sur les réseaux, des *modems*, les puces *RFID* (*radio frequency identification*), les logiciels, etc.

On considère ici qu'est « cyber » tout ce qui a un lien avec les ordinateurs, l'informatique, les réseaux, *Internet*, et que le cyberspace est un « espace virtuel » contenu par les ordinateurs ou entre eux dans le cas de mise en réseau »⁽⁴⁾. Mais cette approche est insatisfaisante. La liste, nécessairement incomplète, s'apparenterait rapidement à un inventaire à la Prévert.

L'une des méthodes les plus fréquemment utilisées pour décrire cet objet technique (infrastructures matérielles, programmes, protocoles) mais néanmoins empreint d'une dimension littéraire, onirique voire romantique non négligeable (le cyberspace est le lieu de la virtualité, du rêve, de tous les possibles, la source d'un monde potentiellement meilleur), demeure le recours à la métaphore, à l'analogie : le cyberspace, lieu virtuel, abstrait, est ainsi comme une page blanche sur laquelle on calque les caractéristiques du monde connu. Nombre de représentations graphiques utilisent l'image du globe terrestre⁽⁵⁾, des étoiles, de l'espace interstellaire, des galaxies⁽⁶⁾, pour imager la complexité du système « cyberspace ». La notion de « *cloud computing* » est l'emprunt le plus récent au monde aérien. Les pirates informatiques (*hackers*) dont la tête de mort sur fond noir est le symbole évoquent, quant à eux, le monde marin : un *Internet* liquide, sur lequel navigue l'internaute. La ville est également au centre des métaphores : rappelons-nous les cités virtuelles dans lesquelles évoluent les protagonistes de films comme *Matrix* ou *Hackers*, où des murs de données constituent ceux des immeubles ou des pièces des bâtiments. Le cyberspace est aussi une « forteresse digitale »⁽⁷⁾. Entre ces univers (villes, continents), se dressent des océans de données, se tracent des routes (outil « *tracer* »), se construisent les « autoroutes de l'information ».

Plus intéressante nous semble-t-il est l'approche systémique : l'*Internet* est décrit comme un système complexe, ensemble de systèmes adaptatifs, victime de « virus » tout comme peut l'être le corps humain, autre système complexe. Les ordinateurs, les réseaux sont des corps infectés, malades, qui révèlent leurs faiblesses. Des projets de cartographie de l'*Internet* proposent souvent des représentations rappelant la structure du cerveau⁽⁸⁾. Si l'ordinateur peut être considéré comme un cerveau, la mise en réseau de tous les ordinateurs constitue un méga-cerveau, *Internet*, le cyberspace. Dès lors, mener des cyberattaques, c'est attaquer le cerveau de la société moderne, son système nerveux, son épine dorsale : les cyberattaques peuvent devenir une menace vitale pour le système qu'est la société⁽⁹⁾.

Dans le vocabulaire militaire, cyberspace et spectre électromagnétique sont souvent associés. C'est l'idée exprimée par exemple par le général William T. Lord, commandant de l'*Air Force Cyberspace*

(4) Cf. lien (<http://dictionnaire.phpmyvisites.net/definition-cyberspace-11421.htm>).

(5) Exemple (www.blueboat.fr/wp-content/uploads/2008/06/tag-galaxy-2.jpg).

(6) Représentation de Walrus (www.nicolas-guillard.com/cybergeography-fr/atlas/walrus2_large.gif).

(7) Titre du roman de Dan Brown.

(8) Cf. lien (www.nicolas-guillard.com/cybergeography-fr/atlas/lumeta_large.jpg).

(9) *National Strategy to Secure Cyberspace*, février 2003 (www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf).

(10) *Cyber War: Preparing Combat Forces for the Electromagnetic Spectrum*, avril 2008 (www.blacklistednews.com/view.asp?ID=6187).

(11) Voir par exemple : *The National Military Strategy for Cyberspace Operations (NMS-CO)*, Chairman of the Joint Chiefs of Staff, Washington D.C., décembre 2006.

(12) Voir par exemple : *JP 1-02*, États-Unis, 12 avril 2001, définition p. 110 ([www.bits.de/NRANEU/others/jp-doc-trine/jp1_02\(01\).pdf](http://www.bits.de/NRANEU/others/jp-doc-trine/jp1_02(01).pdf)).

(13) Voir *JP 1-02*, version 2001 ([www.bits.de/NRANEU/others/jp-doc-trinejp1_02\(01\).pdf](http://www.bits.de/NRANEU/others/jp-doc-trinejp1_02(01).pdf)), définition p. 231. La définition est reprise dans la version amendée du document du 13 juin 2007 (p. 294).

(14) *National Security Presidential Directive 54, Homeland Security Presidential Directive 23* (NSPD-54/HSPD-23).

(15) *Cybersecurity Act*, 2009, USA.

(16) « *Cyberspace Operations, Air Force Doctrine Document 3-12* », USAF, juillet 2010.

Command, lorsqu'il affirme que le cyberdomaine recouvre « l'intégralité du spectre électromagnétique »⁽¹⁰⁾. Le document de doctrine AFDD 3-12 de juillet 2010 de l'*USAF* précise que les segments du cyberspace sont connectés et supportés par une infrastructure physique, des systèmes électroniques et des portions du spectre électromagnétique. Pour les militaires et le gouvernement américains, le cyberspace est tantôt qualifié de domaine⁽¹¹⁾, tantôt d'environnement⁽¹²⁾, de nouvelle dimension⁽¹³⁾, d'infrastructure⁽¹⁴⁾, de processus⁽¹⁵⁾. Il n'est surtout pas un bloc homogène, uniforme. Il faut au contraire distinguer des milliers de cyberspaces⁽¹⁶⁾.

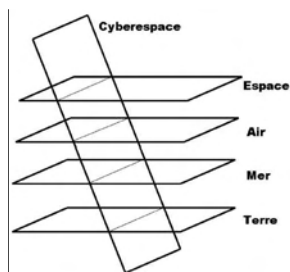
Modéliser le cyberspace

Comme sous-ensemble de l'espace informationnel

Si le cyberspace est le lieu de l'information, il n'est pas celui de toutes les informations et données produites. Deux individus peuvent échanger des propos sans que jamais ceux-ci n'entrent dans l'espace de l'information numérisée ; un écrit papier, le son produit par un instrument, sont des données et de l'information qui peuvent être communiquées (un émetteur, un récepteur) sans qu'il y ait de relation au cyberspace. Nous considérons que le cyberspace est un sous-ensemble de celui, bien plus large, que l'on nommera espace informationnel. Le cyberspace crée ses propres données/informations, et se nourrit de celles de l'espace informationnel.

La transversalité

Si le cyberspace est la 5^e dimension du combat, il n'est pas parallèle aux quatre dimensions conventionnelles (terre, mer, air, espace) mais leur est plutôt transversal : il traverse, croise en effet les dimensions conventionnelles, sans jamais les recouvrir totalement. Le cyberspace innerve chacune des dimensions du réel mais ne les recouvre pas toutes totalement. Le schéma 1 offre une vue de cette transversalité.



Lorsque nous regroupons (par commodité méthodologique) les dimensions conventionnelles en une seule, nous obtenons la dimension du réel (R), qui se trouve croisée par la dimension virtuelle, le cyberspace (V). Cf. schéma 2.

Schéma 1 - Le cyberspace, dimension transversale aux quatre espaces conventionnels.

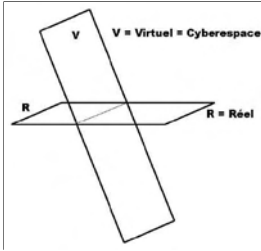


Schéma 2 - Le cyberspace (V) est transversal au Réel (R).

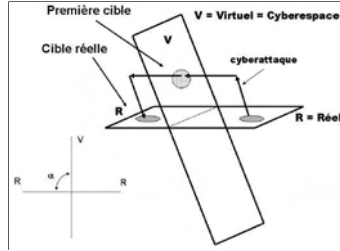


Schéma 3 - Les cyberattaques dans le modèle de la transversalité.

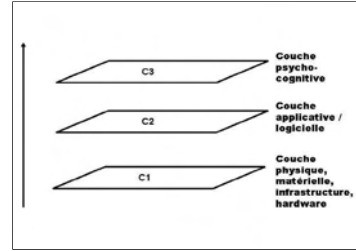


Schéma 4 - Représentation des 3 couches constitutives du cyberspace.

Cette représentation simplifiée de la position du cyberspace par rapport aux autres dimensions permet par exemple de définir les cyberattaques comme des opérations agressives de R à R passant par V. Cyberattaque et cyberdéfense ont pour objet, partant de R, de produire un impact/effet dans R. Et V n'est finalement qu'un vecteur, un filtre, un milieu dans lequel on agit. La cyberattaque utilise V, qui n'est que la cible première. La véritable cible est R et la force de l'impact, l'effet produit, est essentiellement fonction de la vulnérabilité de la cible finale, c'est-à-dire de la qualité de sa relation à V ; ce qui est symbolisé par l'angle alpha dans le schéma 3.

Structure en 3 couches

Le cyberspace, cet espace qualifié précédemment de « virtuel », peut être décrit comme une structure composée de trois couches interdépendantes les uns des autres : une première couche matérielle, physique, celle des infrastructures, du *hardware* mais aussi du spectre électromagnétique (C1 dans le schéma 4) ; une seconde couche logicielle, applicative (C2) ; une troisième couche dite couche cognitive ou psycho-cognitive (C3).

En s'appuyant sur cette représentation, le cœur des cyberattaques repose sur une manipulation de la couche intermédiaire mais on comprend qu'une action sur l'une d'entre elles produit un effet sur les autres. Quelques règles peuvent être définies.

- Chaque couche implique des acteurs, des cibles et des objectifs spécifiques (la couche inférieure peut relever de la guerre électronique, celle intermédiaire de la cyberguerre, la couche supérieure de la guerre de l'information, dans sa dimension opérations d'informations/*Psyops*).

- Si les cyberattaques peuvent toucher chacune des couches (une attaque logicielle peut perturber le fonctionnement au niveau de la couche physique et avoir un impact en C3), la cyberdéfense doit impérativement englober les aspects techniques (programmation) mais aussi cognitifs, politiques, psychologiques, industriels. Aucune couche ne saurait être traitée de manière isolée. La cyberdéfense comme la cyberattaque peut imposer de recourir à un spectre de compétences, d'acteurs de secteurs différents (fournisseurs d'accès, opérateurs de télécoms, fournisseurs de technologies ont leur rôle à jouer au même titre que les programmeurs, les *think tanks*, les « hacktivistes »).

- Les actions sur les couches peuvent être combinées.

On peut ainsi agir sur C1 (couper des câbles *Internet* sous-marin, détruire des satellites de communication/observation...) pour produire un effet sur C2 (impossibilité d'utiliser les réseaux) et/ou C3.

On peut agir sur C2 (piratage, intrusion, défiguration de site...) pour produire un effet sur C3 (déstabiliser) et/ou C1 (une attaque virale peut détruire des systèmes, des ordinateurs...).

On peut agir sur C3 (diffuser des listes de cibles potentielles) pour produire un effet sur C2 (des *hackers* passent à l'action) avec de possibles implications en C1.

On peut lancer une action simultanée sur C1 et C2 pour obtenir un effet sur C3.

Tableau 1 - Association de chaque couche à ses acteurs, actions et considérations théoriques

		Caractéristiques	Forme d'attaques possibles contre la couche	Faits	Perspective théorique
C3	Couche haute	Couche cognitive	Modifier l'affichage des ordinateurs, défigurer des sites, introduire des messages modifiant les perceptions, mener des opérations de propagande, <i>hacking</i> cognitif	Défigurations de site, « hacktivisme », <i>WikiLeaks</i> , utilisation des réseaux sociaux pour mobiliser des foules. Une attaque contre la couche cognitive consiste à manipuler les contenus pour manipuler les acteurs.	<i>Netwar</i> (Arquilla, Ronfeldt), guerre de l'information (Libicki), opérations psychologiques, opérations d'information, influence
C2	Couche médiane	Couche applicative : logiciels, applications, couche des <i>bits</i> , du code, des normes, des protocoles, les données	Attaques par le code : <i>hacking</i> , diffusion de virus...	Défiguration de sites, « hacktivisme », piratage de serveurs de ministères, intrusions, attaques <i>DDoS</i> , vols de données...	<i>Cyberguerre/cyberwar</i> . La couche C2 est au cœur de la notion de cyberguerre.
C1	Couche basse	Couche physique, matérielle : <i>hardware</i> , câbles, réseaux, satellites, ordinateurs, matériels communiquant, infrastructures connectés	Couper des câbles sous-marins, détruire des satellites, détourner des satellites de leur trajectoire, bombarder des bâtiments accueillant des serveurs, bombarder des infrastructures de communication, employer des bombes <i>EMP</i> ...	Coupure de câbles sous-marins paralysant l' <i>Internet</i> en Égypte.	Les actions au niveau de cette couche peuvent ainsi relever de la guerre électronique (<i>EW</i>), plus généralement des simples opérations cinétiques, mais être menées par le biais de C2 et donc d'actions logicielles (<i>Stuxnet</i>).

Ce simple modèle à 3 couches permet par exemple de distinguer les priorités de cyberdéfense chinoise et américaine : la Chine semble avant tout préoccupée par les atteintes contre C3, quand les États-Unis paraissent se montrer plus sensibles aux atteintes en C2 et C3.

Le cyberspace : matrice 3 x 4 ?

En combinant l'approche transversale et le modèle à trois couches, nous construisons une matrice de dimension 3 x 4.

	Terre	Mer	Air	Espace
C3				
C2	X	X	X	X
C1	X	X		X

Tableau 2 - Cyberspace : 3 couches, 4 dimensions

Nous utilisons la matrice de la manière suivante :

- il y a du C1 sur terre (réseaux, câbles, ordinateurs), dans les mers (câbles sous-marins par exemple), dans l'espace (satellites) ;

- il y a du C2 dans les 4 dimensions (du logiciel embarqué dans les avions, les satellites, les navettes spatiales...) ;

- la dimension psycho-cognitive est rattachée à l'individu qui peut être présent dans chacune des 4 dimensions conventionnelles ; les contenus peuvent traiter de ces quatre dimensions ;

- pour obtenir un effet sur C3 une action peut être menée dans {C1 : mer} (couper un câble sous-marin) ou {C1 : Espace} (détourner un satellite de sa trajectoire par des moyens logiciels pourrait être un moyen de démonstration de force susceptible de modifier la perception d'une menace).

Cadre de recherche de la cyberstratégie

Olivier Kempf | Maître de conférences à Sciences Po, conseiller de rédaction de la *Revue Défense Nationale*. Il est l'auteur de *Stratégies dans le cyberspace* (avec Stéphane Dossé, Éditions L'esprit du livre, 2011) et de *Introduction à la cyberstratégie* (Économica, prévu en octobre 2012). Il dirige la collection « Cyberstratégie » chez Économica.

Un colloque * tenu le 29 novembre 2011 a rassemblé, pour la première fois à Paris, des spécialistes (professionnels, chercheurs, étudiants, responsables divers) de la cyberstratégie : il faut ici entendre le mot comme la couche supérieure des études de cybersécurité. Les échanges, fructueux, ont permis d'esquisser un cadre de recherche des études de cyberstratégie.

Chacun a pu constater qu'un mot a traversé tous les débats : celui d'ambiguïté. En fait, le cyberspace donne l'impression d'être celui des réalités fluides et floues. C'est cette ambiguïté qui rend le sujet difficile à cerner et en fait donc un passionnant sujet de pensée stratégique. Au fond, nous nous trouvons face au « fait cyber » comme les premiers stratégestes face à l'irruption du fait nucléaire : cette profonde nouveauté nécessite de reconsidérer l'ensemble du spectre stratégique.

Pour cela, la réflexion stratégique peut être orientée selon un certain nombre de champs de recherche. On peut en dénombrer dix principaux, avec toutes les limites que comporte ce type de découpage.

L'étude des limites

La notion de limite paraît essentielle pour appréhender ce cyberspace.

Et tout d'abord, la question de la définition qui a suscité de nombreuses interrogations et des commentaires très partagés. Cyberspace, est-ce le bon mot ? Il faut ici décrire une certaine gradation : sécurité des systèmes d'information (SSI), cybercriminalité, cybersécurité, cyberdéfense, cyberguerre, sachant qu'on ne sait s'il faut parler de cyberguerre ou de guerre informatique. Il faut également examiner la question de la frontière. La distinction entre espace physique et espace virtuel constitue la première frontière. Mais il y a aussi des frontières géographiques qui marquent donc des souverainetés : il faut apercevoir le paradoxe de la territorialisation géographique du milieu cyber, malgré son apparence d'extraterritorialité. La « mutabilité » paraît constituer un autre mot utile pour appréhender les limites : dans le cyber, les armes

* Colloque « Le cyberspace, nouveau domaine de la pensée stratégique », organisé par le Centre de recherche des Écoles de Coëtquidan et Alliance géostratégique à l'École militaire. Actes à paraître chez Économica.

et outils sont mutables et donc rien n'est fixe ni établi. Les instruments du cyber sont mouvants : non seulement ils se meuvent mais en plus, ils mutent. Ils peuvent changer à la fois de position mais aussi de nature : leur caractérisation et donc leur description sont d'autant plus ardues. Cette mutabilité des agents se réfléchit sur l'ensemble du système, qui devient lui-même mutable, transformable. Du coup, il faut évoquer les mots de dualité, d'intrication et d'imbrication : la dualité a plusieurs formes, elle est bien évidemment civilo-militaire mais elle réside aussi à l'intersection entre public et privé, entreprise et citoyen, intérieur et extérieur...

La dualité est multiple, ce qui rend difficile la définition des limites. Peut-être faut-il d'ailleurs définir les limites avant de décrire les lieux, à l'inverse de la méthode traditionnelle des naturalistes qui décrivent pour, peu à peu, analyser, regrouper puis synthétiser. Toutefois, cette dualité permet une conclusion partielle qui peut être appréciée favorablement : le cyber est peut-être dual mais cela permet une continuité d'action qui n'est pas forcément handicapante, notamment en termes sécuritaires.

Le cyber comme espace

L'interrogation sur la notion d'espace rejoint partiellement la question des frontières.

Le cyberspace est-il un milieu comme les autres ? En tout état de cause, constatons qu'il est anthropogène, créé par l'homme, artificiel au sens premier. Cela pose la question de la machine mais aussi de l'humain. Cette humanité renvoie donc à l'aspect social de ce milieu : il n'est pas « en soi » mais par rapport à des acteurs, et on relira avec bienfait *Le réseau et l'infini*, de Polycarpe et Forget ⁽¹⁾ qui s'interrogeaient déjà sur la question.

Partons de la supposition que le cyberspace est un milieu stratégique en soi : il faut donc rechercher les principes propres à ce milieu. Ce peut être une énumération qui inclurait par exemple sûreté, résilience, surprise, contournement, rupture, coalescence, chaos, rhétorique, la liste n'étant pas limitative ⁽²⁾.

Le cyberspace n'est pas un milieu clos, il interagit avec les autres milieux (espace terrestre, maritime, aérien, exo-atmosphérique, électromagnétique, nucléaire...). On en déduit le besoin d'étudier la combinatoire des milieux car qui dit stratégie dit qu'on ne peut pas rester dans un seul milieu. S'il y a une loi stratégique, c'est celle de l'empilement de ces milieux donc de leur interaction. Le cyberspace est également un espace émetteur, récepteur, et donc transitaire de stratégies inter-milieux. On ne peut se contenter d'observer le seul

(1) Philippe Forget et Gilles Polycarpe, *Le réseau et l'infini*, essai d'anthropologie philosophique et stratégique, Économica, bibliothèque stratégique, 1997.

(2) Voir Stéphane Dossé et Olivier Kempf, « Les principes stratégiques du milieu cyber » in *Stratégies dans le cyberspace*, Éditions L'esprit du livre, 2011.

cyberespace, il faut le penser dans sa dynamique stratégique avec d'autres milieux.

Cette approche par les milieux entraîne la question des modèles et de ce qu'on peut en tirer. On a beaucoup parlé du nucléaire, notamment sous l'angle de la dissuasion, la comparaison étant très discutée en France alors qu'elle est prônée aux États-Unis. À propos du nucléaire, il faudrait également interroger la justesse de la notion de « pouvoir égalisateur » qui pourrait peut-être être transposée de l'atome au cyber. On a tenté une comparaison avec le modèle terrestre, en s'inspirant de la lecture de Beaufre. Une autre comparaison vient également des Américains, il s'agit des *Global Commons* (espaces communs : mer, air, espace, cyberespace), qui renvoie à la notion d'espace fluide : le cyberespace est-il l'équivalent d'un espace maritime ou de l'espace exo-atmosphérique ? Ne faut-il pas aller imaginer un espace propre qui réunit des caractéristiques stratégiques isolées de tel ou tel milieu ?

Le cyber est enfin un espace organisé : n'obéit-il pas à un modèle fractal ? Ou encore, sa structure ne ressemble-t-elle pas à un hologramme ? En tout état de cause, on sent bien que tout le macro descend très vite au niveau micro, ce qui renforce la difficulté de penser stratégiquement le cyberespace : au fond, qu'est-ce qu'un « réseau » ? Et tout d'abord, est-il forcément plan comme nous en avons l'intuition ou n'est-il pas épais ?

Pour conclure cette partie, il faut insister sur la couche physique sous-jacente au cyberespace. Elle est susceptible de faire l'objet d'actions physiques sur tel ou tel de ses éléments : détruire des infrastructures (agglomérats de serveurs, *data centers*, nœuds, câbles, refroidisseurs, approvisionnement électrique) fait partie de la cyberstratégie. Autrement dit, l'action dans le cyber passe aussi par des destructions physiques et des frappes directes.

Le cyber et le temps

Après l'espace, il faut interroger le temps. En fait, le cyber est un cyberespace-temps.

Le cyberespace est le lieu d'une extrême fugacité et de l'instantanéité (fulgurance). Les opérations électroniques vont à la vitesse de l'électron, avec des durées inférieures à la nanoseconde.

Cela pose la question de l'anticipation : est-on seulement dans l'instant ? N'est-on pas aussi dans la longue durée ? Le rapport au temps est donc extrêmement variable. L'anticipation, supposée nécessaire, induit la question du renseignement et celle de la constitution de dossiers d'objectifs avant action. Mais comme ils sont opaques, discrets, camouflés, ils présupposent une certaine conflictualité plus ou moins acceptée. En fait, pour permettre la fulgurance, il faut probablement une action préventive, ce qui relève de la décision stratégique : elle est d'autant plus stratégique qu'elle est occulte et que

seul le décideur politique peut, en fin de compte, la choisir. Il faut de fait penser une chronostratégie du cyber. Cela renvoie à la notion de permanence. Nous devons assurer une permanence de la gestion de la cybercrise. Cette permanence stratégique doit être analysée à l'aune d'un concept connexe, qui peut faire l'objet d'études propres, celui de la résilience : en matière cyber, la résilience est-elle une fonction d'abord temporelle ou plus technique ?

Le dernier sujet lié au temps tient au rapport de la planification et de l'automatisme : le contrôle humain de la réponse demeure-t-il possible ? L'homme a-t-il le temps de « contrôler » ? Pour autant l'automatisme, de l'ordre de la nanoseconde, n'est-il pas perturbateur (qu'on pense aux robots financiers qu'on est obligé de débrancher car ils déstabilisent le système qu'ils observent) ? La brièveté de l'action cyber pose ainsi la question du contrôle stratégique : en anglais, on traduit « commandement » par « *Command and control* ». Commander c'est contrôler, ce qui renvoie à l'aspect social et humain du cyberspace précédemment mentionné.

Le cyber et la gouvernance

La gouvernance dépasse la place de l'État même si celle-ci est cruciale.

Elle pose tout d'abord la question du droit. En effet, le droit de référence doit-il être national (utilisation de la notion de légitime défense, pertinence du droit pénal) ou international (adaptation de la Charte des Nations unies, nécessité d'un traité *ad hoc*, éventuelle codification des normes existantes...) ? Par ailleurs, à l'instar d'autres domaines stratégiques, le cyberspace pose les questions de la qualification de l'acte de guerre mais aussi de l'attribution de l'acte. Autrement dit, le *corpus* d'un droit de la cyberguerre autonome doit être envisagé, utilisant les outils d'autres domaines juridiques et développant ses instruments adaptés.

Il reste que ce sera probablement l'État qui sera à la source de ce droit, qu'il soit national ou international. Il faut alors interroger son rôle. Est-il acteur, coordonnateur, cible, animateur ? Quel doit être son centrage : seulement autour du ministère de la Défense, en interministériel, sur un spectre plus étendu, selon quelles configurations ? Les organes en place (ministère de la Défense, ANSSI) suffisent-ils ? Comment concevoir en la matière l'intérêt national, voire l'intérêt vital (notion fondamentale en termes de dissuasion nucléaire, faut-il le rappeler) ? Et quelle mise en œuvre de ces concepts faut-il envisager, avec quelle marge d'ambiguïté ?

L'extension du rôle de l'État renvoie à la question des libertés publiques dont la nécessaire préservation peut s'opposer aux exigences de sécurité et de protection (d'autant qu'*Internet* se présente comme « libre et gratuit ») : constatons toutefois qu'assez tôt après l'invention de l'automobile, on a inventé le permis de conduire que personne ne voit aujourd'hui comme une vraie atteinte à la liberté de circulation. Mais la cyberdéfense pose

indirectement la question de la légitime défense ou de l'autodéfense au niveau du citoyen, et celle de la régulation que l'État doit y apporter. C'est la reprise d'un débat ancien qui oppose l'action publique ayant pour objet la sécurité aux libertés individuelles qu'il faut protéger, dans leur principe comme dans leur exercice.

Cyberespace et dimension internationale

L'État n'a pas que des rapports avec les citoyens, il en a aussi avec la communauté internationale. Cela renvoie à la question de la collaboration internationale : quel est le cadre pertinent (ONU, G20, Otan, UE, Quinte, bilatéral) ? Quelle souveraineté l'État doit-il se réserver, selon des régimes envisageables de discrétion, de partage ou de confiance ? De ce point de vue, l'analogie avec les pratiques de coopération en matière de renseignement semble féconde. Cette coopération internationale pose aussi la question de la régulation. On pense à la question de la maîtrise des armements. La comparaison avec les autres traités de maîtrise des armements devrait permettre de déterminer si une telle orientation est possible en matière cyber et selon quelles modalités. Ce qui nous amène à la question des procédures et de la standardisation dans ce cadre international : est-ce forcément un bien ? Quelle utilité, quelle utilisation, quelle instrumentation ? La standardisation peut en effet être technique et économique, avant d'être légale et publique.

Enfin, la dimension internationale du cyber amène à appréhender sa géopolitique particulière : tout d'abord, il faut examiner les éventuels rapports du cyber au territoire et l'éventuel isolement international de celui-ci par décision nationale. Il s'agit également d'analyser les dimensions cyber des conflits existants et leur instrumentation par la diplomatie ou tout autre dialogue plus ou moins ouvert. Enfin, on interrogera les rapports de force existants, grâce notamment à une typologie encore à conduire autour des principaux acteurs et de leurs alliances possibles : à titre d'exemple, peut-on envisager une alliance des États-Unis avec la Russie contre la Chine ? Quel rôle pourrait jouer des acteurs alternatifs comme l'Inde ou Israël ? Les pays émergents ne peuvent-ils pas se saisir de ce nouvel espace stratégique pour installer une position relative de puissance ? (US/Russie face à Chine ? Inde ? Israël ? Émergents ?). Les scénarios et cas d'espèce sont nombreux et méritent une grande attention.

Considérations stratégiques

L'analyse géopolitique conduit naturellement à des considérations stratégiques. Elle est aujourd'hui, sous l'influence des Américains, beaucoup influencée par la notion de dissuasion, comme nous l'avons déjà noté. De ce point de vue, les esprits français sont dépendants de leur culture stratégique. En France, la dissuasion est forcément nucléaire, ce qui n'est pas le cas aux

États-Unis et entraîne probablement certaines confusions. Toutefois, si on pense la dissuasion d'une façon générale, donc comme une intimidation, elle renvoie à la définition de la stratégie, celle de la dialectique des volontés, pour reprendre les mots du général Beaufre.

Cette dialectique est tout d'abord une dialectique entre des actions défensives et des actions offensives. Celles-ci font désormais partie de la gamme des outils à la disposition du décideur. Mais dans le milieu incertain et opaque qu'est le cyber, cela pose la question de l'initiative : selon un vocabulaire stratégique traditionnel, faut-il envisager des actions préventives (qu'il est d'usage de condamner) ou préemptives (qui constituent un cas particulier de la légitime défense, avec à la fois des indices clairs et une imminence d'action de l'adversaire, et qui sont donc admises) ?

C'est au fond la question de l'emploi de ces armes qui est posée : emploi, non-emploi, là encore l'analogie avec le nucléaire vient à l'esprit, même si l'on a un peu oublié qu'en matière nucléaire, le non-emploi était une conséquence, non un principe ⁽³⁾. Il reste que cette question de l'emploi des cyberarmes demeure pendante, et pour certains « personne ne franchira le Rubicon ».

(3) Olivier Kempf, « Dissuasion du fort au faible », *Revue Défense Nationale*, février 2012.

Une autre dimension stratégique tient au secret des opérations, qui est légèrement différent de la question des procédures de renseignement (aspect plus tactique et technique des choses) : en effet, stratégiquement, le secret pose la question du masque, de la surprise, de la clandestinité, de la dimension discrète et subreptice de l'action. La sienne mais aussi celle de l'autre : immédiatement, voici posé le grand sujet de l'attribution. Mais alors que trop souvent, on n'y voit qu'une contrainte technique, il serait peut-être possible de retourner la vulnérabilité : la nôtre est aussi celle de l'autre, l'attaque permet la défense. Au fond, il s'agit d'inverser l'asymétrie supposée entre soi et l'adversaire : supposée, car ce vocabulaire stratégique (symétrie, dissymétrie, asymétrie) nécessite d'être utilisé pour comprendre les possibilités cyberstratégiques. Au fond, il faut décrire l'ensemble des postures stratégiques possibles selon l'acteur considéré.

Ce rapport des acteurs ne doit pas pour autant obérer la dimension technologique. Il y a ainsi une dialectique technologique, qui repose notamment sur le rapport de l'arme et de la cible. Il semble que la cible détermine la construction de l'arme ; il faut confirmer cette idée et en examiner les conséquences stratégiques. Car cela détermine l'éventuel pouvoir égalisateur du cyber et l'équilibre de la terreur numérique : là encore, on reconnaît un vocabulaire qui appartient à celui de la dissuasion nucléaire mais qui mérite d'être précisé et adapté aux particularités de ce nouveau milieu.

Dispositifs opérationnels

À supposer qu'il y ait « cyberguerre », celle-ci ne se réduit pas aux considérations stratégiques, elle passe aussi par des dispositifs opérationnels.

La structure des réseaux a longtemps laissé croire que l'on pouvait se contenter d'une défense périmétrique. Toutefois, les dispositifs actuels en maillage laissent entrevoir la possibilité de « défense dans la profondeur » qui favoriserait la posture défensive, ce qui reste à démontrer. De même, ces dispositifs doivent viser la protection mais aussi la résilience : tout défenseur sait que son dispositif pourra être localement percé mais que son système doit être globalement résilient pour rétablir au niveau macro une déficience constatée au niveau micro. Pour cela, des thèmes comme le combat en essaim, la dissémination, l'étude des dégâts collatéraux, la gestion du chaos seront d'intéressants sujets d'études.

Il est également probable que l'étanchéité d'un réseau constitue la meilleure parade : autrement dit, la non connexion avec l'extérieur serait la meilleure garantie, même si elle induit des coûts car elle encourt le risque de la duplication : ces réseaux internalisés et non connectés constituent en fait des réseaux privés. Toutefois, ils reposent sur des infrastructures générales (faisceaux, réseaux électriques) qu'il ne faut pas omettre dans l'analyse.

Tout conflit de demain aura forcément une dimension cyber. Il faut donc considérer les aspects de télécommunications et d'informatique mais aussi les liens avec la numérisation de l'espace de bataille (NEB), avec le renseignement électronique (*ELINT-SIGINT*), avec la guerre électronique (GE), à la suite de ce qu'on a nommé « le combat cyberélectronique ». Tout ceci est-il fondu ou doit-on garder des distinctions ? Pour dire les choses autrement, faut-il une fusion du cyberspace et de l'espace électromagnétique ? Quelles conséquences opérationnelles cela entraîne-t-il ? Les aspects opérationnels de ces cyberconflits posent par ailleurs plusieurs questions : celle de la coordination des efforts par le chef interarmes (y a-t-il une manœuvre de niveau opératif ou tactique ? Y a-t-il commandement ou contrôle ? Quel rôle donner à l'échelon central et/ou stratégique ?). Par ailleurs, le renseignement comporte forcément une dimension cyber (veille informative, intelligence informative) à laquelle il faut plus réfléchir.

Enfin, il pourra être opportun, à l'heure de déterminer les modes d'action, de comparer à d'autres modes opératoires : on peut penser à la guerre biologique (virus et propagation) mais aussi à la guerre des mines (pollution localisée d'un espace fluide, minage et déminage). Cela conduit à la question du « mode dégradé » : comment agir et survivre dans un cyberspace dégradé ? Est-ce possible ? Quelles procédures envisager ?

Sens et information

La guerre cyber ne doit-elle considérer que les aspects technologiques ? Rappelons la distinction à faire entre les stocks, les flux et les sens, ceux-ci constituant la dernière couche du millefeuille cyber, la couche lexicale, au-dessus des couches physique et logique. Le cyberspace est un espace organisé en vue de supporter cette couche sémantique. L'information n'est pas qu'une « donnée » (au sens que les mathématiciens et les informaticiens donnent à ce mot), elle est orientée et polarisée.

Cela amène à la question de l'influence : c'est-à-dire des actions indirectes mais aussi des opérations d'information. Elle inclut une rhétorique (un peu comme dans la stratégie nucléaire). À ceci près qu'il faut s'interroger sur la dimension cachée de nos actions : avons-nous intérêt à dire ce qu'on fait et à évoquer nos actions ? Faut-il pour autant ne rien dire ? Quels niveaux d'ambiguïté devons-nous choisir ? Dans cette même veine, il faudra réfléchir à l'articulation entre la notoriété et la crédibilité mais aussi aux possibles emplois de la mystification, de la déstabilisation, de la rumeur. Il s'agit bien sûr là de catégories anciennes de l'art de la guerre et on se gardera d'oublier que le « stratagème » a la même étymologie que le stratège : mais justement, en quoi cette nouvelle technique favorise-t-elle de nouveaux dispositifs de déception ?

Une autre question, soulevée incidemment lors de ce colloque, tient à la dimension éthique des actions dans ce cyberspace : est-il possible de tout faire ? Cela dépasse la simple question du droit et renvoie, d'une façon générale, à la problématique de l'artificialisation du champ de bataille, qu'on observe par exemple en matière de drones ou de robots.

Ainsi, faudra-t-il articuler les différents résultats de cette recherche stratégique dans un *corpus* doctrinal : depuis l'apparition de la dissuasion nucléaire, on sait désormais que la part rhétorique de l'action stratégique doit être traduite dans des concepts et des doctrines, qui seront l'expression du sens.

Cependant, cette recherche ne pourra faire l'économie d'une approche philosophique et épistémologique de la modernité : on pense ici aux travaux sur la cybernétique (N. Wiener, Mandelbrot), sur la systémique (Bertalanffy, G. Bateson, H. Simon), sur la complexité (Morin, Le Moigne), qui sont d'ailleurs dès l'origine liés à l'émergence du cyberspace : revenir sur les notions de globalité et d'incertitude constitue, à n'en pas douter, un axe de recherche fécond pour les stratégestes.

Stratégie et technologie

Le cyberspace est un milieu artificiel, nous l'avons suffisamment souligné. Ce qui signifie qu'il est structurellement dépendant de la technologie. Nous n'entrerons pas dans le détail des développements envisageables et de

leurs conséquences prévisibles : qu'on rappelle juste qu'au début des années 1970, Motorola expérimente les premiers prototypes de téléphone portable. Mais les experts ne croient pas au développement de ce marché. À la fin des années 1970, une étude du cabinet McKinsey estimait qu'en 2000, il n'y aurait au mieux que 900 000 abonnés. Il y en eut 120 fois plus ⁽⁴⁾ ! Cet exemple illustre, si besoin était, que la prévision des conséquences technologiques est aléatoire. Souvenons-nous qu'à la sortie du premier processeur Pentium, certains analystes s'interrogeaient sur l'utilité d'une telle puissance. Aujourd'hui, le moindre « téléphone intelligent » a plus de puissance de calcul que les premiers Pentiums. Il y a ainsi une course technologique dont on ne peut prévoir les conséquences.

(4) Philippe Silberzahn, « Entrepreneurat, risque et incertitude » (philippesilberzahn.com), 11 avril 2001, accédé le 9 janvier 2012.

Toutefois, on peut s'interroger sur certaines permanences, qui structurent la réflexion. Évoquons-en trois, bien conscient que bien d'autres mériteraient d'être étudiées.

La première semble tenir à l'opposition entre ouverture (ou liberté) et sécurité : en plus de la question de gouvernance déjà évoquée, la question sous-jacente est celle du modèle technologique mais aussi de son coût. C'est un peu ce qu'on attend de l'IP v6 ou du nouveau protocole américain sécurisé. Les choix d'architecture détermineront les réponses stratégiques.

La seconde est celle de la prolongation des courbes : autrement dit, poursuivra-t-on la loi de Moore, qui prévoit un doublement régulier (à rythme constant) de la capacité de calcul ? Cela sous-entend qu'il y a une barrière physique. Pourquoi pas, mais n'y a-t-il pas des contournements technologiques envisageables ? Et si oui, lesquels, dans quelle direction ?

La troisième s'interroge sur la ressource physique sous-jacente à ce nouvel espace : plus que la loi de Moore, ne faut-il pas craindre une barrière énergétique ? Quelle empreinte carbone le cyberspace a-t-il ? Quelles conséquences faut-il voir sur la géopolitique des ressources et n'y a-t-il pas de rétro-effets stratégiques sur ce milieu ?

Ces questions restent ouvertes, parmi d'autres.

Économie

Les liens entre le cyber et l'économie sont nombreux. D'emblée et d'un point de vue stratégique, il faut tout d'abord s'interroger sur les liens entre le cyber et la guerre économique. Constatons d'ailleurs que cette dernière souffre, elle aussi, des mêmes difficultés conceptuelles que « la cyberguerre » : on a du mal à la définir et on sent bien, simultanément, qu'il y a là un champ conflictuel

qui ressort, peu ou prou, de la guerre. Il reste que cette guerre économique d'un genre nouveau prend sa signification depuis l'espace mondialisé apparu dans les années 1990, et de façon synchrone au développement de ce qu'on nommait alors les « nouvelles technologies de l'information et de la communication ». La mondialisation économique tire sa source non seulement d'une dérégulation commerciale ou d'une augmentation des échanges mais aussi de la facilité permise par les nouveaux outils informatiques, que ce soit pour les échanges (financiers ou commerciaux) ou pour la gestion des flux. Or, cette mondialisation est le théâtre d'une guerre économique et il paraît plus que pertinent d'examiner comment les États mais aussi les entreprises utilisent le cyberspace pour la mener. C'est toute la question de la sécurité économique des entreprises, de leur intelligence stratégique et leur cyberintelligence.

Le prisme économique amène ensuite à penser la question de la gratuité : quel modèle économique d'*Internet* faut-il promouvoir ? La question renvoie à celle de la gouvernance ; mais alors que celle-ci opposait les libertés individuelles à la sécurité collective, on voit bien que dans le cas économique, on oppose une liberté individuelle à un monopole privé. La privatisation économique du cyber (*via* des droits de péage) permettrait la création de monopoles, même s'il faut envisager la constitution de systèmes alternatifs et « libres », comme l'émergence récente de la « pirate-box » l'illustre ⁽⁵⁾. La puissance publique est régulatrice et intervient souvent au nom de l'intérêt commun. Qu'il soit permis de penser qu'elle doive aussi le faire en fonction de considérations stratégiques. Notons au passage que l'éventuelle apparition d'acteurs majeurs, quasi monopolistiques, dans le cyberspace posera la question de l'écosystème à encourager (ou pas) entre les industriels d'armement et les industriels du cyber. De même, le cyber suppose une « logistique » de son milieu qui doit être pensée, là aussi en termes opérationnels.

(5) Notons au passage que la lutte économique entre le consommateur « libre » et le monopole privé a des conséquences politiques, comme l'illustre le succès des partis pirates en Europe du Nord et en Allemagne.

Enfin, on peut observer un autre exemple de ces liens entre liberté du consommateur et liberté du citoyen. En effet, la logique initiale d'expansion du cyber (sa diffusion maximale) a conduit à négliger la sûreté des systèmes : combien cela coûterait-il de reconstruire un système plus sécurisé (notamment dans les noyaux) ? La sécurité globale a un coût économique qu'il faut tout d'abord évaluer mais aussi attribuer : qui paiera ? Le citoyen par ses impôts, le consommateur par ses achats, l'entreprise par ses marges ?

Autres questions stratégiques liées au cyber

Pour terminer, évoquons quelques thèmes qui ne sont pas entrés « naturellement » dans les catégories déjà évoquées. Cela ne

signifie pas qu'ils ne sont pas importants, simplement que le domaine est neuf et mérite d'être défriché.

On pense ainsi à un sous-thème, qui pourrait certainement être avantageusement étudié : celui de ce qu'on appellera les « transgressions », même si le vocabulaire n'est peut-être pas le plus opportun. On évoquera ici les rapports entre le terrorisme et le cyber ou entre la criminalité et le cyber. D'une façon plus générale, il s'agit de réfléchir au renouvellement contemporain des révoltes et leur association à ce cyberspace : indignés, *Anonymous*, *Wikileaks*, *LulzSec*, voici autant de signes d'une nouvelle pratique de la révolte qu'il faut étudier sous un angle stratégique ⁽⁶⁾.

(6) Ce sujet a d'ailleurs été traité lors du colloque « Se révolter au XXI^e siècle », organisé par le club Participation et Progrès et l'École de Guerre Économique le 14 mai 2012. Actes à paraître en 2013.

Le deuxième thème est celui des nouveaux rapports de force : qu'on pense ici aux relations entre le cyber et la notion d'émergence ou à l'instrumentalisation stratégique des réseaux sociaux (regardons de plus près l'action des États-Unis dans les révoltes arabes). Ici encore, le champ d'étude est large et mériterait de nombreux développements.

Il y aurait d'autres thèmes d'études en friche et je ne doute pas qu'ils émergeront.

**

Ce colloque posait une question simple : le cyberspace est-il un nouveau domaine de la pensée stratégique ? Incontestablement, la réponse est positive ! Il s'agit d'un champ d'étude très vaste avec, dès à présent, de multiples directions de recherche. Nous avons essayé d'esquisser les principales, en faisant confiance à la communauté stratégique pour en préciser les contours et les lignes de force. Il est probable que ce travail s'organisera par des relations entre le flou et le flux.

Pour terminer d'un point de vue stratégique, retenons l'importance de la vulnérabilité. La nôtre est aussi celle de l'adversaire, puisque nous partageons les mêmes vulnérabilités : attention au tropisme défensif, celui de l'Occidental craintif et apeuré assiégé dans sa forteresse : il faut penser lucidement notre situation pour justement définir une ligne stratégique calculée. Surtout, cela permet de revenir sur la stratégie indirecte, évoquée en citant le général Beaufre. Le cyberspace est, à bien des égards, un magnifique espace de stratégie indirecte, celui où l'intelligence peut le mieux se manifester : ce qui est rassurant car, s'il n'y a pas forcément de pouvoir égalisateur du cyber, au moins peut-on espérer dans un pouvoir égalisateur de l'intelligence.



Les hommes et les choses

Un homme ouvre, à l'occasion, un tiroir longtemps délaissé. Il y découvre une montre qu'il y avait déposée et dont le souvenir même l'avait quitté. Il la prend, l'examine, s'en souvient, constate qu'elle tourne et que l'heure qu'elle affiche est juste. Depuis quelques mois, donc, bonne montre, bonne pile, elle poursuivait dans l'ombre son travail, matérialisant le temps qui passe. Pour personne. Imagine-t-on sort plus triste que celui de cette montre consciencieuse, ignorée des humains pour lesquels elle travaille ?

Un autre homme, ou le même, parcourt, à dos de chameau et bien droit sur sa selle, les solitudes de l'Est mauritanien, mer de dunes blondes que, faute de puits, seuls les plus rustiques des chasseurs nomades sont capables d'affronter. Rien ne s'offre au regard du voyageur que le déferlement des sables, trop volatiles pour que quelque végétation s'y accroche. Soudain, au pied d'une dune plus haute qui protège en son creux un sol plus ferme, apparaît une plaque d'herbe tendre dont la verdure, frémissant sous la brise légère, se dore aux rayons du soleil matinal. L'homme se repaît du spectacle et sa monture, tête aussitôt baissée, goûte la saveur de la plante qu'on appelle *telebout* et dont il n'est pas de plus succulente. L'homme et sa bête eussent-ils dévié leur route d'un angle infime, la miraculeuse rencontre n'aurait pas eu lieu et ce minuscule trésor de vie et de beauté, disposé là par la grâce d'Allah, serait resté solitaire, à jamais non regardé.

La montre et l'herbe du désert, ensemble nous interpellent : l'homme est-il fait pour voir les choses, les choses sont-elles faites pour être vues par l'homme ? Si telle est la loi de nature, les choses non regardées sont inutiles, leur existence non justifiée. Ô désespoir des choses jolies que nul regard, jamais, n'effleurera ! Mais allez savoir ! Cet anthropocentrisme n'est pas du goût de Gilles Lapouge :

« Je pense, dit la baronne, que toutes les choses de la terre, elles continueront à être là, et même quand nous dormirons au cimetière. C'est ce que je me dis toujours, quand je suis au bord de la mer et au bord des larmes. Je me dis que les vagues continueront à faire leur fourbi même quand il n'y aura plus personne pour les entendre. Plus jamais personne, dans un million d'années je veux dire, elles feront le même bruit exactement. Elles sont comme ça, les vagues, elles sont comme de bons soldats, et de penser à ces choses-là, c'est curieux, c'est comme si j'étais heureuse » ⁽¹⁾.

Le Vieil

(1) Gilles Lapouge : *La légende de la géographie* ; Albin Michel, 2009.

L'usage de la force dans le cyberspace et le droit international

Loïc Simonet | Docteur en droit et fonctionnaire au ministère de la Défense. Il s'exprime ici à titre personnel.

(1) On fera nôtre la définition de la cyberattaque qu'offre Davis Brown : "The term 'information attack' means the use of computer and/or other information or communications systems to destroy, alter, or manipulate data or images, engage in denial-of-service attacks, transmit malicious code, or perpetrate similar attacks, or do physical damage to any target, for the purpose of inflicting injury or degrading the enemy's ability or will to fight" ("A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict", *Harvard International Law Journal*, vol. 47, n° 1, hiver 2006, p. 215).

(2) Sylvain Cypel, Le Pentagone pourrait assimiler les cyberattaques à des 'actes de guerre' ; *Le Monde*, 3 juin 2011, p. 5.

(3) *Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, Section 934, novembre 2011, p. 4.

(4) "Deter and Defeat Agression" (*Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*), Département de la Défense, Washington D.C., 5 janvier 2012, p. 4).

(5) *Department of Defense Cyberspace...*, op. cit., p. 2.

(6) *Livre blanc sur la défense et la sécurité nationale*, Paris, Odile Jacob-La Documentation française, juin 2008, p. 207.

(7) "Cyber supporting fire" (général Keith B. Alexander, in "Building a New Command in Cyberspace", *Strategic Studies Quarterly*, été 2011, vol. 5, n° 2, p. 5).

Le 28 mai 2011, Lockheed Martin, le géant américain de la défense, annonçait avoir repoussé une attaque « significative et tenace » menée par des *hackers* qui étaient parvenus à dérober des codes d'accès à l'un de ses fournisseurs. Quelques heures après cette cyberattaque ⁽¹⁾, des responsables de l'armée américaine annonçaient que de tels actes, dans la mesure où ils provoqueraient la paralysie ou la destruction partielle du fonctionnement de l'État, de l'économie nationale ou des systèmes civils collectifs, seraient désormais considérés comme des « actes de guerre », ouvrant la voie à une riposte militaire de même nature que celle que s'attirerait une attaque armée. Largement répercutée par les médias occidentaux ⁽²⁾, cette nouvelle doctrine américaine était consacrée, quelques mois plus tard, par le Département de la Défense américain ⁽³⁾.

C'est donc dans le cyberspace, au même titre que sur terre, sur mer ou dans les airs, que l'armée américaine situe désormais sa capacité à dissuader et à mettre en échec une « agression » ⁽⁴⁾. Elle réagira aux actes hostiles dans le cyberspace « de la même façon » qu'elle le ferait pour toute autre menace affectant les États-Unis, après avoir, lorsqu'elle le pourra, épuisé les autres options « avant l'usage de la force » ⁽⁵⁾.

Comme l'avait parfaitement théorisé le *Livre blanc*, « la planification et l'exécution d'opérations combinées avec des actions cybernétiques tendent (...) à devenir la norme. Avant même que des cibles physiques ne soient détruites, tout système de défense pourra être en effet désorganisé et partiellement aveuglé par des frappes silencieuses et ciblées » ⁽⁶⁾. C'est par un véritable « tir de soutien » informatique ⁽⁷⁾ qu'ont été précédées les opérations aéroterrestres de l'armée russe contre la Géorgie, en août 2008, traduisant une convergence évidente entre les intentions des auteurs de cette attaque et les actions de l'armée russe. Cet épisode atteste que les cyberopérations « deviennent une véritable tactique au service d'un objectif

militaire »⁽⁸⁾. Les cyberarmes sont donc en passe de devenir des moyens de combat efficaces utilisables dans une situation de conflit, sans avoir recours aux systèmes d'armes traditionnels.

Bien qu'il ne soit pas évident de faire coïncider la volatilité et l'immatérialité du cyberspace et les critères du droit international, les actes que l'on vient de mentionner doivent-ils être soumis à cette matière, et notamment au droit des conflits armés ? *"It will not be as easy to apply existing international law principles to information attack"* : ce constat prudent dressé par les experts juridiques du département de la Défense américain, s'impose en effet rapidement au juriste⁽⁹⁾. Ce n'est pourtant pas la première fois que le droit international doit affronter l'émergence de nouvelles technologies susceptibles de faire peser une menace sur la sécurité internationale. Dans son avis consultatif du 8 juillet 1996, la Cour internationale de justice (CIJ) avait eu à répondre à la question suivante, posée par l'Assemblée générale des Nations unies : « Est-il permis en droit international de recourir à la menace ou à l'emploi d'armes nucléaires en toute circonstance ? »⁽¹⁰⁾.

L'usage de techniques de cyberdéfense au cours d'un conflit conventionnel ne pose guère de questions : il s'agit de l'usage d'une arme, d'une technique militaire parmi d'autres, fut-elle « nouvelle » au sens du premier Protocole additionnel aux Conventions de Genève. En revanche, la question de savoir si l'acte d'hostilité dans le cyberspace, en lui-même et indépendamment d'un conflit préexistant, relève de l'« usage de la force » ou représente un « acte d'agression »⁽¹¹⁾, a d'importantes implications en droit international : elle commande en effet une possible réaction sur le fondement de la légitime défense, malgré la difficulté que pose le rattachement de l'auteur de la cyberattaque aux autorités de l'État.

Une cyberattaque relève-t-elle de l'usage de la force ? Constitue-t-elle un « acte d'agression » ?

Selon le premier Protocole additionnel, « l'expression "attaques" s'entend des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs »⁽¹²⁾. À première vue, la cyberattaque semble entrer dans le champ de cette définition : le général Keith Alexander, responsable du *US Cyber Command*, peut donc, à juste titre, estimer que la cyberattaque massive dont a été victime l'Estonie, en 2007, a confronté l'Otan et ses nations à une véritable « attaque armée » dans le cyberspace⁽¹³⁾ ; d'autant que la CIJ a eu l'occasion de rappeler que l'interdiction générale de l'emploi de la force édictée par la Charte des Nations unies, ne préjugait pas de l'usage « d'armes particulières » et s'appliquaient « à n'importe quel emploi de la force,

(8) Jean-Loup Samaan, « Les trois âges de la cyberdéfense américaine », *Les carnets du cap*, ministère des Affaires étrangères et européennes, Direction de la Prospective, printemps-été 2011, n° 4, p. 127.

(9) *Office of General Counsel, "An Assessment of International Legal Issues in Information Operations"*, Department of Defense, mai 1999, p. 5.

(10) *Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif*, C.I.J. Recueil 1996, paragraphe 1, p. 228.

(11) Nils Melzer, *Cyberwarfare and International Law*, 2011, Institut des Nations unies pour la recherche sur le désarmement (Unidir), collection Ressources, Genève, 2011, p. 22 et ss.

(12) Art. 49 du Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), du 8 juin 1977 ; on s'est référé au texte du Protocole tel qu'il figure sur le site du CICR (www.icrc.org/).

(13) Général Keith B. Alexander, *op. cit.*, p. 5.

(14) *Licéité de la menace ou de l'emploi d'armes nucléaires*, *op. cit.*, § 39, p. 244.

(15) Nils Melzer, *op. cit.*, p. 7. C'est la raison pour laquelle la cyberattaque menée contre l'Estonie en 2007 aurait difficilement pu, même si elle avait conduit à l'incrimination d'un État étranger (ce qui n'a finalement pas été le cas), déboucher sur des représailles armées car la perte d'aucune vie humaine n'a heureusement été déplorée.

(16) On se réfère ici à la version publiée sur le site de l'ONU (www.un.org/fr/).

(17) *"In terms of the UN Charter, it is clear that a range of information attacks would constitute uses of force, and a comparable range of countermeasures would constitute legitimate self-defence"* (Gregory D. Grove, Seymour E. Goodman et Stephen J. Lukasik, *"Cyber-attacks and International Law"*, *Survival*, vol. 42, n° 3, automne 2000, p. 100).

(18) Cf. la clause d'assistance mutuelle de l'Union européenne « Au cas où un État-membre serait l'objet d'une agression armée sur son territoire, les autres États-membres lui doivent aide et assistance par tous les moyens en leur pouvoir, conformément à l'article 51 de la Charte des Nations unies » (art. 42 paragr. 7 du Traité sur l'Union européenne, version consolidée, *Journal officiel de l'UE*, C83, 30 mars 2010, p. 39).

indépendamment des armes employées »⁽¹⁴⁾. Même si le débat continue d'animer les juristes, on peut donc estimer que des attaques informatiques pourraient relever de l'usage de la force selon la Charte, à condition toutefois que les effets de ces actes soient comparables, en termes de létalité et de destructions, à ceux d'attaques conventionnelles ou NBC (nucléaires, biologiques ou chimiques)⁽¹⁵⁾. Une fois admis que la cyberattaque peut relever de l'usage de la force et constituer un acte d'agression, comment y répondre sans violer l'interdiction générale de recourir à la force posée par le droit international ?

La réponse à une cyberattaque peut-elle relever de la légitime défense ?

En 1945, les promoteurs de la Charte de San Francisco⁽¹⁶⁾ n'avaient nullement à l'esprit qu'advierait un jour une société de l'information. C'est la raison pour laquelle ses dispositions ne s'appliquent qu'imparfaitement, et au prix de quelques contorsions intellectuelles, aux cyberattaques transnationales.

L'article 51 de la Charte consacre le « droit naturel de légitime défense, individuelle ou collective, dans le cas où un membre des Nations unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales ». Toutefois, le recours à l'article 51 pour justifier des actions de cyberdéfense soulève au moins deux questions.

D'une part, il implique que soit définie la notion d'« agression armée », beaucoup plus restrictive que celle de « l'emploi de la force » dans le fameux article 2, paragraphe 4 de la Charte, puis qu'elle soit mise en relation avec les particularités d'une cyberattaque.

D'autre part, l'article 51 prévoit que : « Les mesures prises par des membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité » ; or, la prise de contrôle du réseau par des moyens extrêmement sophistiqués et confidentiels paraît peu compatible avec cette obligation de publicité.

Sous ces réserves, il est de plus en plus communément admis que la légitime défense collective de l'article 51 permet de justifier le recours à la force en réaction à une cyberattaque⁽¹⁷⁾. Une telle opinion est d'importance car elle entraîne avec elle les clauses de solidarité dont les États-membres de plusieurs systèmes d'alliance se sont dotés et qui se fondent sur l'article 51⁽¹⁸⁾. On sait que l'Estonie, estimant faire face à une réelle agression, avait un temps envisagé en

2007 d'invoquer l'article V du Traité de l'Atlantique Nord. Cependant, le juriste bute ici immédiatement sur un problème propre au cyberspace : la difficulté, si ce n'est l'impossibilité, d'établir un lien entre les auteurs d'une cyberattaque et les autorités d'un État.

Comment concilier le droit international et la difficile imputabilité de la cyberattaque à l'État ?

On sait l'importance, en droit international, de la question du contrôle de l'État sur ses ressortissants, à laquelle la jurisprudence a apporté une réponse hésitante. Comme l'atteste l'épisode de 2007 en Estonie, dans lequel le rôle direct des autorités russes n'a jamais pu être indubitablement prouvé, il est souvent malaisé d'attribuer la responsabilité d'une attaque dans un cyberspace sans frontières, ce qui rend difficile une contre-attaque ou des mesures de représailles ⁽¹⁹⁾. Même si l'on parvient à localiser dans un pays l'origine d'une attaque, il est difficile de déterminer si l'agresseur a agi à titre individuel ou au nom d'une organisation criminelle, du gouvernement ou des forces armées. En particulier, les agissements d'« hacktivistes » sur le territoire d'un État ne peuvent systématiquement conduire à l'incrimination de ce dernier ; l'utilisation de codes volés ou l'usurpation d'identité informatique peuvent faire croire à la responsabilité d'un État qui n'y est en réalité pour rien, ce qui multiplie potentiellement les risques d'« escalade » si cet État est mis en cause de manière injustifiée : on imagine ce qu'eussent été les conséquences d'une invocation de l'article V du Traité de l'Atlantique Nord par l'Estonie contre la Russie, comme cet État avait pensé le faire en 2007, alors que l'enquête allait finalement aboutir à l'incrimination d'un citoyen estonien, certes d'origine russe.

Hormis les situations claires d'offensives informatiques précédant une intervention armée (cas du conflit russo-géorgien d'août 2008), le rôle de groupuscules difficilement identifiables et dont le rattachement à des autorités étatiques est souvent malaisé, rend difficile l'appréhension de la cyberdéfense par le droit international. « La guerre symétrique est morte », constate le général Desportes ⁽²⁰⁾ : en ce sens, la guerre informatique est « asymétrique » par nature, puisqu'elle oppose à l'État et à ses institutions un « attaquant » difficile à identifier et à confondre. Pour reprendre l'expression imagée mais parlante de W. Lynn, un missile balistique touche sa cible avec une « adresse de réexpédition » : l'État sur le territoire duquel il a été tiré s'expose à des représailles immédiates ; il n'en est pas de même du virus informatique ⁽²¹⁾.

Or, la définition de l'« agression » en droit international renvoie à l'État ⁽²²⁾ ou à l'une de ses émanations ⁽²³⁾. L'acte d'agression reste donc un « acte de l'État » ⁽²⁴⁾.

(19) De même, l'implication de pirates informatiques tolérés et contrôlés par les autorités chinoises, voire de l'armée populaire de libération elle-même, a été évoquée lors des attaques qui ont visé, en 2007, le ministère français des Affaires étrangères ; mais le gouvernement chinois a démenti tout lien avec ces événements et indiqué lui-même confronté aux agissements de ces pirates (*rapport d'information du Sénat sur la cyberdéfense*, par M. Roger Romani, n° 449, annexe au procès-verbal de la séance du 8 juillet 2008, p. 9-10).

(20) Vincent Desportes, *La guerre probable*, Paris, Économica, 2007, p. 29.

(21) « *Whereas a missile comes with a return address, a computer virus generally does not* » (William J. Lynn III, « *Defending a New Domain. The Pentagon's Cyberstrategy* », *Foreign Affairs*, vol. 89, n° 5, sept.-oct. 2010, p. 99).

(22) « L'agression est l'emploi de la force armée par un État contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre État » (définition de l'agression en annexe de la résolution 3314 (XXIX) de l'Assemblée générale des Nations unies, en date du 14 déc. 1974, consultée sur le site de l'ONU (www.un.org/)).

(23) « On entend par 'crime d'agression' la planification, la préparation, le lancement ou l'exécution par une personne effectivement en mesure de contrôler ou de diriger l'action politique ou militaire d'un État, d'un acte d'agression », art. 8 bis du Statut de Rome de la CPI, tel qu'amendé en 2010 par la conférence de Kampala sur la révision du statut (www.icc-cpi.int/).

(24) Cf. Maurice Kamto, *L'agression en droit international*, Paris, Pédone, 2010, p. 11 et ss.

Cette difficulté d'identification des auteurs d'une cyber-attaque pourrait cependant ne pas être un obstacle absolu au déclenchement de représailles armées. Les juristes du Pentagone, s'appuyant sur l'exemple des frappes américaines contre les camps d'entraînement de terroristes en Afghanistan en août 1998, avaient envisagé qu'une action en légitime défense préventive puisse être engagée sur le territoire d'un État qui démontrerait son incapacité ou son absence de diligence à mettre fin aux agissements de cyberterroristes ⁽²⁵⁾. Dans un tel contexte, on peut penser qu'un simple faisceau de présomptions sérieuses et concordantes pourrait suffire à déclencher cette action préventive, précédée de sommations et de mises en demeure adressées à l'État négligent.

**

En conclusion, le cyberspace met en évidence l'inadéquation des normes classiques du droit international. On peut même se demander si la notion de « territoire », pourtant fondamentale en droit international (elle est notamment constitutive de l'État), possède encore un sens. Comme l'évoquait un juriste, « le cyberspace n'est nulle part » ⁽²⁶⁾.

Le droit international n'est certes pas dépourvu de toute capacité de réponse face aux activités dans le cyberspace. Comme on vient de le voir, de nombreuses dispositions du droit des conflits armés trouvent un écho dans cet univers virtuel. Pour autant, la transposition de principes et de normes préexistants ne s'opère pas sans ambiguïtés et l'on peut se demander si la communauté internationale pourra faire l'économie d'un *corpus* juridique spécialement consacré à ce phénomène. Il est donc probable que les instruments et la doctrine du droit international, et notamment l'interprétation de la Charte des Nations unies, devront évoluer pour prendre en compte l'« usage de la force » dans le cyberspace, comme le préconisait le rapport du Sommet mondial sur la société de l'information, en 2003 ⁽²⁷⁾. Les efforts du Centre d'excellence de l'Otan à Tallinn, en faveur de l'élaboration d'un manuel sur le droit de la guerre dans le cyberspace (*Manual on the International Law of Cyber Warfare*), pourraient y contribuer de manière significative ⁽²⁸⁾.

« La cybervulnérabilité est un concept au bel avenir », observait un théoricien de la doctrine militaire ⁽²⁹⁾. Nul doute que cet avenir croisera celui du droit international.

(25) “Only if the requested nation is unwilling or unable to prevent recurrence does the doctrine of self-defense permit the injured nation to act in self-defense inside the territory of another nation” (Office of General Counsel, *op. cit.*, p. 22) ; cf. le rapport du département de la Défense au Congrès, qui envisage une telle possibilité d'action sur le territoire d'États tiers, dans certaines conditions (*op. cit.*, p. 8).

(26) “Cyberspace is nowhere” (Davis Brown, *op. cit.*, p. 180). De même, la notion de neutralité de certains États ne représente plus grand chose dans le cyberspace : pour simplifier, on pourrait dire que nul État n'est neutre au regard d'Internet. Or, l'État neutre doit traditionnellement s'abstenir de toute activité en lien direct avec le déroulement des hostilités et les belligérants doivent s'abstenir d'utiliser son territoire.

(27) “Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar”, *International Centre for Scientific Culture*, rapport et recommandations, document WSIS-03/Geneva/Contr/6-E, 19 nov. 2003, p. 30. Ce même rapport suggérait que la Commission du droit international des Nations unies se voit confier la tâche d'élaborer un cadre juridique approprié qui définirait notamment les situations dans lesquelles des cyber-actions « légitimes » pourraient être menées par les États (p. 31).

(28) On renverra également à l'intéressant projet de convention élaboré par Davis Brown, *op. cit.*, p. 215 et ss.

(29) Vincent Desportes, *op. cit.*, p. 174.

Agir et réagir dans le cyberspace

Vincent Joubert | Chercheur associé, Observatoire de géopolitique, Chaire Raoul-Dandurand en études stratégiques et diplomatiques – UQAM.

Il n'est plus question aujourd'hui pour les grandes puissances d'ignorer l'importance stratégique du cyberspace. Colonne vertébrale des sociétés modernes, il est également un domaine extraordinairement fragile dont la protection constitue cependant un enjeu primordial. Ce constat impose alors de penser les moyens de protéger ses intérêts dans un espace en perpétuelle évolution, toujours plus complexe.

Le cyberspace, parent pauvre de la pensée stratégique française ?

Bien que le cyberspace soit un domaine « jeune », la cyberstratégie n'a bénéficié en France que d'une attention tardive. Longtemps réservé presque exclusivement aux informaticiens qui traitaient des questions de sécurité des systèmes et des réseaux, le champ ouvert à la stratégie militaire par le cyberspace a rapidement conduit à des réflexions sur les enjeux et les capacités stratégiques du domaine ainsi constitué. En France, s'il est évoqué dans le *Livre blanc* en 2008, il n'est pas une priorité pour la Défense. Quelques auteurs abordent le sujet mais celui-ci semble rester réservé aux « connaisseurs ». Aux États-Unis, *a contrario*, les premiers travaux sur le sujet remontent au début des années 1990 ⁽¹⁾ puis se sont multipliés avec les innovations technologiques laissant entrevoir des applications militaires attrayantes, pour devenir dès 2008 un sujet prioritaire à la Maison-Blanche et au Département de la Défense.

Paradoxalement à cet intérêt tardif pour les implications stratégiques du cyberspace, les enjeux sécuritaires liés à la protection des intérêts nationaux par la sécurisation des systèmes et réseaux ont conduit la France à développer un ensemble de moyens institutionnels et opérationnels qui lui confèrent aujourd'hui le statut de « cyberpuissance » de premier plan. L'intérêt grandissant des puissances pour le sujet a ensuite attisé les curiosités et poussé un nombre croissant de personnes concernées par les questions de défense à s'intéresser aux règles stratégiques propres à ce domaine et à sa relation

(1) L'article le plus fameux est celui de J. Arquila & D. Ronfledt, "Cyberwar is coming!", *Comparative Strategy*, Vol. 12, n° 2, printemps 1993, p. 141-165.

à la stratégie générale. Aujourd'hui, le cyberspace reste un territoire où la réflexion stratégique française est à ses balbutiements mais les enjeux et les défis créés par ses spécificités techniques et technologiques sont tels qu'ils stimuleront sans peine les échanges et débats intellectuels.

Parmi les nombreuses problématiques du sujet, il est une réflexion nécessaire à mener sur la façon de se faire respecter dans le cyberspace, notamment par l'utilisation de capacités offensives, *COC* (*Cyber Offensive Capabilities*) et sur leur place dans les stratégies de cyberdéfense. Elle ouvrira le champ à la mise en place d'une stratégie de dissuasion dans et par le cyberspace.

Le champ d'application des *COC* : possibilités et limites

Les capacités offensives dans le cyberspace ou cyberarmes, peuvent être définies comme « l'ensemble des programmes informatiques utilisés ou élaborés pour être utilisés dans le but de menacer ou de porter atteinte à l'intégrité physique, au fonctionnement ; ou psychologiquement, à des structures, des systèmes ou des êtres humains »⁽²⁾. Actuellement, les *COC* peuvent être utilisées dans deux cas de figure :

- Dans un but offensif. Ici, un État utilisera ses *COC* pour attaquer un adversaire dans et/ou par le cyberspace. Ces actions offensives regroupent plusieurs types de cyberattaques, destructrices ou non-destructrices, selon l'objectif recherché.

Par exemple, des *COC* peuvent être employées à un niveau opérationnel, s'inscrivant dans le cadre d'une stratégie plus large, qui utilise de manière coordonnée l'ensemble des outils militaires. Typiquement, elles serviront à neutraliser ou dégrader des capacités de défense ou de ravitaillement adverses afin de faciliter la progression de ses propres forces militaires. Ce fut le cas en 2007, lorsque la défense antiaérienne de la Syrie fut neutralisée par Israël pour permettre à son aviation de détruire sans encombre un site de construction d'un centre nucléaire⁽³⁾. Ce scénario, dans lequel des *COC* permettent de dégrader les systèmes de l'adversaire, est le plus redouté par les États-Unis en cas de conflit avec la Chine, notamment dans le détroit de Taïwan⁽⁴⁾.

Les *COC* peuvent également être employées dans le cadre de « *covert actions* », dans un but spécifique et limité. Le virus *Stuxnet*, qui infecta en 2009 des logiciels d'automates industriels utilisés dans la centrale nucléaire iranienne de Natanz et retarda *in fine* le programme d'enrichissement d'uranium iranien d'une année, en est un exemple. En dépit d'une absence de revendication officielle, la

(2) Thomas Rid & Peter McBurney, "Cyber-weapons", *The RUSI Journal*, 157, 1^{er} février 2012, p. 6-13. Notre traduction.

(3) Cet épisode, baptisé *Operation Orchard*, a été analysé en détail par un éditorialiste du magazine américain *Aviation Week*. On pourra aussi se référer à l'article de Charles Bwele, 2010 (<http://alliancegeostrategique.org/2010/10/04/raid-cyber-israel-syrie/>).

(4) Voir entre autres M. Libicki, *Chinese Use of Cyberwar as an Anti-Access Strategy: Two Scenarios*, RAND Corp., janvier 2011.

(5) Pour une analyse détaillée de *Stuxnet*, voir N. Fallière, L. O. Murchu, E. Chien, "W32. *Stuxnet* Dossier", *Symantec*, 2011 ; sur la probable origine israélo-américaine du programme (www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=4&pagewanted=all).

sophistication du programme laisse à penser qu'un ou plusieurs États ont méticuleusement préparé cette opération ⁽⁵⁾. Enfin, les *COC* peuvent être utilisées pour des actions de cyberespionnage. Elles peuvent avoir des objectifs politiques, commerciaux, militaires. La facilité de leur mise en place ainsi que les pertes financières associées à la compromission de systèmes ou d'informations en font la pratique la plus problématique à ce jour.

- Dans un but défensif. On peut envisager différentes utilisations des *COC* pour défendre ses réseaux et systèmes.

Avant une attaque. On pose ici la question de l'action préemptive dans le cyberspace, où surgissent les mêmes problématiques que dans les domaines physiques : nécessaire mise en place préalable de mécanismes de surveillance de l'adversaire pour détecter les signes avant-coureurs de l'attaque, évaluation stratégique et politique de l'intérêt à agir de façon préemptive dans le cyberspace, capacités à utiliser pour asseoir sa crédibilité stratégique sans dévoiler l'étendue de ses *COC*, cible à viser pour atteindre l'objectif recherché...

Pendant une attaque. On est ici au cœur de la « défense proactive » qui veut protéger les systèmes et réseaux en mettant hors-service les ordinateurs à l'origine de l'attaque à l'aide de *COC*. Cette défense active, voulue par une majorité d'experts aux États-Unis, s'oppose à la défense passive ou réactive, comparée en matière d'efficacité à la Ligne Maginot pendant la Seconde Guerre mondiale. Cette position pose toutefois des défis techniques – il faut arriver à remonter à la source de l'attaque, évaluer les défenses du système, choisir l'attaque adaptée qui le mettra hors-service, le tout sans abîmer les systèmes et réseaux tiers utilisés à leur insu pour mener l'attaque et dans un délai suffisamment court pour rester dans une action de défense proactive et non de représailles ⁽⁶⁾. La défense active repose actuellement en grande partie sur la résilience des systèmes ; les *COC* viendraient alors compléter ces mesures, palliant les insuffisances des systèmes de protection, sans pour autant empêcher les attaques.

(6) Sur l'importance du délai de réponse, voir M. Libicki, *Cyberdeterrence and Cyber War*, RAND Corp., 2009, chap. 5.

Après une attaque. Pouvoir lancer des représailles dans le cyberspace implique de pouvoir attribuer l'attaque à un acteur. Un ensemble d'indices peut y concourir (techniques, contexte politique, stratégique, etc.) ⁽⁷⁾. Une fois l'attaquant identifié, il faut évaluer l'intérêt stratégique et politique de représailles dans et par le cyberspace. Correspondent-elles au message que l'on veut faire passer ? L'effet recherché sur l'adversaire sera-t-il atteint (par exemple le dissuader de lancer de nouvelles attaques) ?

(7) E. Sterner, "Retaliatory Deterrence in Cyberspace", in *Strategic Studies Quarterly*, printemps 2011, vol. 5, n° 1 ; J. Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks", *Issue Brief, Atlantic Council*, janvier 2012.

Si les *COC* offrent de nouvelles possibilités stratégiques en ajoutant des capacités à l'arsenal militaire, elles souffrent de limites d'ordre technique, juridique et politique.

Sur le plan technique, en plus des complexités déjà évoquées, les cyberarmes oscillent actuellement entre des programmes généraux à faible potentiel destructeur et des programmes spécifiques à fort potentiel ⁽⁸⁾. Chercher à maximiser le potentiel destructeur des *COC* aura alors comme conséquence d'augmenter considérablement les besoins en ressources (financières, renseignements), le temps de préparation, tout en diminuant le nombre de cibles potentielles et donc le rôle politique et stratégique des *COC* ⁽⁹⁾.

Sur le plan juridique, l'applicabilité aux *COC* des droits de la guerre (*jus ad bellum*, *jus in bello*) soulève aujourd'hui beaucoup d'interrogations ⁽¹⁰⁾. La responsabilité des États en cas de cyberattaques (qu'ils en soient la source ou un des relais) attire, elle aussi, les débats. Cependant, les problèmes soulevés ici touchant des sujets sensibles de nature politique (souveraineté des États, secrets de défense, diplomatie, etc.), les questions juridiques sont loin d'être résolues.

Sur le plan politique enfin, la volonté des chefs d'États et de gouvernements d'utiliser les *COC* de manière explicite (hors *covert actions* et cyberespionnage) peut être questionnée, comme l'illustrent les refus américains jusqu'alors, en Irak et en Libye.

La dissuasion par les *COC*

La dissuasion dans le cyberspace fait référence à la dissuasion par représailles. La dissuasion par déni renvoie à la défense des systèmes *stricto sensu*. Suite au constat de l'impossibilité de créer une cyberdéfense autosuffisante, la mise en place d'une dissuasion dans le cyberspace a alors été analysée.

Sujet complexe illustré par de nombreux parallèles faits avec la dissuasion nucléaire pour essayer d'en discerner les points prioritaires : quels sont les outils de l'action offensive créant une barrière dissuasive dans le cyberspace ? Peut-on aboutir à un gel de la volonté de l'autre en le défiant dans son propre cyberspace, comme ce fut le cas avec la dissuasion nucléaire ? Peut-on obtenir des capacités d'intimidation dans le cyberspace pour dissuader l'adversaire et quel parallèle peut-on, là encore, faire avec l'intimidation dans le domaine physique ? Peut-on, par exemple, avoir une panoplie offensive permettant de contrôler l'escalade du conflit – par des coups d'épingle, semonces, arrêts – et qui définiraient par la même occasion des paliers stratégiques de la dissuasion dans le cyberspace ?

(8) T. Rid & P. McBurney, *op. cit.*

(9) *Ibidem.*

(10) Les travaux de M. Schmitt, à ce sujet, font autorité, "Wired Warfare: Computer network attack and jus in bello", *IRRC*, juin 2002, vol. 84, n° 846, p. 365-398.

Si l'analogie décalquée de la dissuasion nucléaire n'est pas pertinente, l'exploitation intelligente des modèles existants dans les domaines physiques (dissuasion nucléaire, conventionnelle, etc.) permettra de mieux discerner les mécanismes sous-jacents à cette stratégie si particulière et de l'appliquer au cyberspace ⁽¹¹⁾.

(11) Joseph S. Nye Jr, "Nuclear Lessons for Cyber Security", *Strategic Studies Quarterly*, hiver 2011, p. 18-38.

Toutefois, aux vues des obstacles techniques empêchant pour le moment la mise en place d'une cyberdissuasion, on peut se demander si les cyberpuissances ne favoriseront pas l'élaboration de circuits fermés de non-agression entre adversaires et partenaires, qui ont appris à se faire respecter après avoir mesuré ce qu'ils savent faire dans le cyberspace ?

Dans ce cas, quelle forme prendraient ces accords de non-agression ? Assisterons-nous à une multiplication d'accords bilatéraux facilitant les échanges et la collaboration, qui semble être la piste privilégiée aujourd'hui ⁽¹²⁾, ou les États privilégieront-ils les cadres internationaux existants (Otan, ONU) pour élaborer un traité international encadrant l'utilisation des *COC* ? Serait-il possible, comme cela a été le cas pour l'arme nucléaire, de créer un « club fermé » entre cyberpuissances afin d'élaborer des intérêts communs ? Cette hypothèse ferait écho à la théorie des jeux développée par T. Schelling, avec un espace neutralisé où les intérêts l'emportent sur l'affrontement et l'isolement. Néanmoins, comme nous l'avons vu, les *COC* peuvent être utilisées à plusieurs niveaux (tactique, opérationnel, stratégique) ; dès lors, on peut se demander quelle portée serait donnée à des accords de non-agression passés par ces clubs fermés ? Quelles utilisations seront bannies, lesquelles se réservera-t-on le droit d'utiliser ? Toutes ces questions sont autant de limites potentielles à la construction d'une dissuasion dans le cyberspace.

(12) Les États-Unis ont par exemple établi des accords sur les questions de cybersécurité avec l'Inde, les Pays-Bas, le Brésil et travaillent à développer des partenariats avec le Japon, le Royaume-Uni, l'Australie, la Corée du Sud et la Nouvelle-Zélande.

*
**

Les capacités offensives cybernétiques, les *COC*, tendent à s'imposer comme outil décisif pour protéger les intérêts et la sécurité nationale dans le cyberspace. Leur utilisation reste pour l'instant cantonnée à des actions qui entrent dans le champ du renseignement (cyberespionnage, *covert actions*) mais les déclarations officielles des cyberpuissances majeures ⁽¹³⁾ montrent que des *COC* seront un outil militaire important dans les prochains conflits. Dans ces conditions, il convient de poursuivre les réflexions stratégiques sur leur impact dans la stratégie générale. Étudier et développer des concepts, des stratégies exploitant au mieux les *COC* permettra de saisir tous les enjeux, les possibilités, les limites, pour mieux agir et réagir dans le cyberspace.

(13) Les États-Unis, la Russie, le Royaume-Uni et la France ont publiquement évoqué l'élaboration de *COC* et leur possible utilisation en cas de conflit futur.



Les gens

Un jour que le Cadet se faisait vanter les mérites d'*Internet* sur son téléphone portable, le vendeur tenta de contrer son scepticisme avec cet argument qui se voulait définitif : vous pourrez consulter les heures des séances de cinéma de Shanghai. Avant que votre serveur n'ait eu le temps de s'enquérir de la manière et surtout de l'intérêt de se rendre le soir même à Cathay pour y voir les mêmes films qu'à Paris, le *quidam* poursuivit : c'est un nouveau monde. Certes, mais dans ce monde forcément global, il y a les gens.

Prenez le film *Wargames* de John Badham qui date de 1982 et qui nous parlait de cyberguerre, déjà. À l'époque les spécialistes s'étaient récriés : on ne peut pas entrer dans l'ordinateur de ciblage des missiles, il y a des sécurités. Trente ans après, on découvre que le principe d'intégration en réseau et l'accessibilité par *Internet* nous permettraient, avec un téléphone et depuis la terrasse d'un café, d'être aussi puissants qu'un Guderian en 1940 mais qu'il est trop tard pour faire machine arrière vu les avantages apportés par ailleurs. Et personne n'avait apparemment pensé qu'il serait beaucoup plus amusant de pénétrer des systèmes de défense que de savoir ce qui est projeté dans les salles à Montevideo.

Alors on palabre, comme à cette chaire de cyberstratégie récemment créée à l'École militaire, où l'on dispute de nouvelles frontières, de nouvelles intrusions et de nouveaux paradigmes, un peu comme si une fois engloutis des milliards dans la Ligne Maginot, on s'était brusquement interrogé du moyen d'éviter que les Allemands ne passent à côté, que dis-je, n'aient l'idée même de la contourner. C'est qu'ils sont contrariants tous ces gens qui savent depuis toujours que lorsqu'on intègre un système on le fragilise suivant le vieil adage qu'une chaîne n'est pas plus solide que le plus faible de ses maillons. Pour un front, un réseau informatique ou une zone monétaire, la meilleure protection reste la structure en grumeaux, la défense ajourée, celle de Vauban et de Séré de la Rivière, celle célébrée par Clausewitz et Liddell Hart. C'est celle de tous les réseaux de résistance, *Anomymous* ou pas. À quand une chaire du bon sens ?

Mais comme le relevait déjà Tocqueville, on théorise sur le progrès du genre humain pour mieux oublier les individus. L'idéal aurait été bien entendu – dystopie totalitaire sans laquelle le principe ne vaut rien – qu'ils cessent de penser. « Mais avec ces gens là, Monsieur », chantait Brel, on n'est sûr de rien. Ah, que le monde serait simple sans eux, sans les chefs *taliban* par exemple qu'un rapport du Pentagone qualifia un jour de *Reluctant participants* !

Et je ne vous parle pas des Grecs, ces autres contrariants qui, tant qu'à crever, préfèrent le faire la tête haute.

Qu'est-ce qu'on passe ce soir dans les cinémas d'Athènes ?

Le Cadet

Advanced Persistent Threats : quelles réponses ?

Sébastien Héon | Directeur des Affaires publiques, Cassidian CyberSecurity.

Les réseaux de communication ont déjà été attaqués à 77 %. Les 23 % restant ne savent pas encore qu'ils vont l'être. Tous les jours, on découvre de nouvelles attaques et de nouvelles compromissions de grande ampleur. Elles touchent tous les secteurs : les institutions nationales, les opérateurs d'infrastructures vitales, les entreprises, petites et grandes. Le *Livre blanc sur la défense et la sécurité nationale* de 2008 était, en ce sens, visionnaire.

Plusieurs exemples récents de ce que l'on appelle les *Advanced Persistent Threats*, les *APT* dans le jargon, révèlent la porosité et la vulnérabilité de nos infrastructures. Ces menaces, plus sophistiquées que des simples virus s'illustrent par un *modus operandi* bien planifié : des ressources humaines qui reconnaissent le terrain, développent des stratégies d'attaques et déploient leurs outils selon un plan d'action construit. Les attaquants, organisés en équipes aux compétences complémentaires, maintiennent dans la durée une présence physique dans les infrastructures pour exfiltrer un maximum d'informations.

Dans la grande majorité des cas, la première étape consiste à envoyer des courriels piégés à une sélection bien choisie de destinataires au sein d'une organisation. Ces courriels pourront s'adresser soit à des employés identifiés à des postes clefs, soit à un ensemble plus vaste de collaborateurs. Les attaquants espèrent qu'au moins un des destinataires ouvrira la pièce jointe, ce qui aura pour effet d'installer un premier programme malveillant. Ensuite, celui-ci téléchargera sa charge utile sur un site contrôlé par les attaquants. De là, ils pourront explorer le réseau informatique à la recherche des informations les plus sensibles : messagerie des hautes autorités, stratégie et données classifiées, et, également pour les entreprises, des informations de R&D, brevets, propriété intellectuelle, informations commerciales... En outre, les attaquants se ménagent plusieurs portes d'entrée et de sortie pour préserver dans le temps leur capacité d'action.

Détection et impacts des *APT* sur les organisations

Ces attaques sont le plus souvent détectées par hasard et très tard. En effet, en moyenne, elles sont découvertes 416 jours ⁽¹⁾ après

(1) www.mandiant.com/threat-landscape/.

leur mise en place. Un petit incident (panne bénigne, dysfonctionnement d'un service informatique...) entraîne l'ouverture d'une investigation qui, progressivement, révélera la présence d'une activité suspecte. Ce n'est qu'après une première analyse de l'informatique interne qu'on en mesurera l'ampleur. Petit à petit, on découvrira qu'un incident anodin cachait la compromission générale du système.

L'attaque dont a été victime le ministère de l'Économie et des Finances en décembre 2010 est emblématique : une détection par hasard puis le constat d'une compromission ancienne et métastasée. Cette crise, bien gérée, a nécessité l'intervention de près de 40 experts pendant 60 jours ce qui représente environ 2,5 M€ de main-d'œuvre. Sans compter le préjudice de la perte d'informations sensibles pour la préparation de la présidence française du G20.

Pour les dirigeants de l'organisation, la prise de conscience des implications que peut avoir le vol de leurs données constitue le moment critique de la crise. Ils réalisent qu'une grande partie de leurs savoir-faire et de leurs investissements de R&D sont désormais en des mains inconnues. Leur responsabilité (pénale éventuellement) pourrait être engagée. Un employé peut se retourner contre son employeur s'il estime que les données à caractère personnel le concernant ont été dérobées. De leur côté, les sous-traitants peuvent également réclamer des dommages et intérêts s'ils s'aperçoivent que ce qui relève de leur propriété intellectuelle a été compromis. Enfin, les dirigeants du secteur privé craignent que la divulgation de l'attaque auprès du public ait un impact négatif en termes de perte d'image et provoque une réaction en chaîne touchant les marchés et les actionnaires. Pour les acteurs du secteur public, la perte de confiance des usagers est préjudiciable. Les dirigeants pressentent également que les *APT* vont avoir un impact majeur sur leur organisation interne car elles remettent en question la place dévolue à la sécurité des systèmes d'information.

Comment réagir au plus fort de la crise ?

Les autorités doivent maintenant prendre les bonnes décisions et se préparer à gérer la crise. Et d'ailleurs, comment fait-on ?

Il faut d'abord résister à la tentation de vouloir « tout débrancher ». La pratique l'interdit généralement : il n'est souvent pas possible d'interrompre ni les opérations en cours ni le système de production. Une fois le choc de la découverte passé, l'étape suivante est l'acceptation de la situation. La plupart du temps, pourtant, la posture de déni constitue un point de blocage important. Les responsables de la sécurité des systèmes d'information, qui font au mieux avec les moyens et les ressources dont ils disposent, sont dans une situation délicate. Comment peuvent-ils expliquer la réalité de la situation à leur hiérarchie sans s'exposer ? Une tendance naturelle est alors de

minimiser la compromission et de prétendre tout solutionner en interne. À ce stade, les dirigeants doivent maintenir la confiance dans leurs équipes de sécurité des systèmes d'information. Mais ils ont également besoin d'un regard extérieur qui saura les conseiller de manière dépassionnée.

Ce tiers de confiance aidera les dirigeants à mettre en œuvre un plan de réaction global, articulé en plusieurs volets. Il commence par une analyse technique conduite par des experts de haut niveau dans les plus brefs délais (c'est une question de jours). Ces derniers investigueront et mesureront l'étendue de l'*APT* grâce à une enquête *forensic* (après intrusion) afin de fournir les éléments suivants : quels sont les canaux d'entrée de l'attaquant, les programmes malveillants mis en œuvre et les sites externes de *command and control* utilisés par les attaquants ? Un aspect fondamental est de savoir sauvegarder les preuves de l'intrusion en vue d'une éventuelle procédure judiciaire. Le tiers de confiance peut assurer, si nécessaire, l'interface avec les autorités nationales compétentes (ANSSI, notamment) à des fins d'information et de soutien éventuel. Ces autorités disposent, en effet, de connaissances approfondies des attaques et d'une grande expérience de gestion d'incident. Il peut, enfin, aider les dirigeants à concevoir un plan de communication interne, voire externe le cas échéant.

Reconstruire le système d'information victime d'une *APT*, une étape nécessaire mais insuffisante

Toute la difficulté est ensuite de reconstruire le système d'information en s'assurant que les programmes malveillants semés par les attaquants ont bien tous été éradiqués. C'est ce que l'on appelle « la bascule ». Les ordinateurs infectés sont reformatés complètement, les canaux d'exfiltration de données sont fermés, les pare-feu reconfigurés correctement, etc. Cette opération de grande ampleur est souvent réalisée dans un laps de temps court (un *week-end*) dans un souci de discrétion et pour surprendre les attaquants. Une fois cette opération réalisée, le système d'information est assaini et quelques-unes de ses vulnérabilités ont été corrigées. Toutefois, si aucune mesure supplémentaire n'est prise, les attaquants ne mettront pas longtemps avant de trouver une nouvelle faille pour s'introduire à nouveau au cœur du système. En effet, 100 % des dernières victimes d'*APT* avaient un antivirus à jour. Les dirigeants réalisent donc que les systèmes d'information comportent des faiblesses structurelles de tous ordres : architecture, manque de supervision dynamique de la sécurité, absence de processus de réaction adéquats et équipes peu ou pas entraînées à la gestion d'incident. Autant de problématiques auxquelles il faut répondre.

Concevoir une architecture de confiance demande une connaissance de l'ingénierie des systèmes d'information, les dernières technologies disponibles avec leurs forces et leurs faiblesses et une capacité à les intégrer dans un environnement métier et opérationnel. Après avoir subi une *APT*, l'architecture

doit être remise en question et améliorée. Pour minimiser les impacts des prochaines attaques qui ne manqueront pas de se produire, il faut les détecter le plus en amont possible et les circonscrire au plus vite. C'est le but de la supervision dynamique qui est conduite par une équipe d'opérateurs organisée pour fonctionner 24 heures sur 24. Elle dispose d'outils de surveillance des réseaux qui corrélient les événements et détecte ainsi les comportements suspects. Les alertes ainsi déclenchées sont analysées et une réponse adéquate proposée. Pour pouvoir réagir efficacement, des plans de réponse doivent être prêts et les équipes doivent être entraînées à les dérouler. Des formations régulières, à tous les niveaux et des exercices sont le gage d'une réaction efficace. Cette activité peut être soit conduite en interne, soit externalisée si l'organisation ne dispose pas des compétences nécessaires.

Bien entendu, ces mesures vont avoir un coût. Certes, l'impact financier d'une attaque reste encore difficilement quantifiable car le sujet est encore peu étudié, les métriques et les statistiques manquent. Il faut prendre en compte le coût des dommages indirects : perte d'image, perte de marchés suite à la fuite d'informations commerciales, perte de compétitivité face à un concurrent qui développe subitement un nouveau produit qui ressemble au vôtre. On estime toutefois qu'il existe un facteur 10 entre les coûts directs et indirects. À cela, il faut ajouter le coût de l'analyse *forensic* et celui de la reconstruction que l'on vient de subir.

Comme dans tous les domaines, la prévention aurait coûté moins cher que la perte de données et la cure de convalescence. Aujourd'hui, les services offerts pour concevoir des architectures de sécurité et superviser les systèmes d'information en temps réel sont abordables et s'adaptent à tous les types et tailles d'organisation.

Prévention et anticipation : une étape indispensable

Les coûts seront d'ailleurs d'autant plus bas que les outils seront sophistiqués et efficaces. Il est donc crucial de maintenir une capacité de développement et d'innovation pour concevoir les sondes de détection, les outils de *forensic* et de diagnostic de demain.

Or, la capacité d'innovation se trouve essentiellement dans les *start-up*. Petites, fragiles, elles n'arrivent pas à trouver seules le marché qui leur permettra de grandir. Elles n'ont pas les moyens de se développer à l'international et restent cantonnées dans un marché de niche de dimension nationale. Elles finissent par périr ou être rachetées par des capitaux étrangers. L'État a un rôle à jouer pour soutenir cette filière industrielle qui est un relais de développement économique : le taux de croissance du marché de la cybersécurité est estimé à plus de 10 % par an sur un volume mondial approximatif de 50 milliards de dollars.

Second axe d'importance pour lequel la puissance publique est un acteur indispensable et fédérateur : la création d'un cercle de confiance. En effet, il faut échanger sur la nature et les *modus operandi* des attaques pour mieux les prévenir et les anticiper. Ces informations sont sensibles par essence. On ne peut partager cette intelligence qu'au sein d'une communauté où chacun est reconnu pour sa connaissance du domaine et son intégrité.

La mutualisation de cette connaissance permet des économies d'échelle en évitant une duplication des efforts de recherche et d'analyse *forensic*. De plus, le partage d'intelligence sur les modes opératoires des attaquants permet une mise à jour itérative des défenses de tous les acteurs.

Enfin, les secteurs publics et privés doivent instaurer des mécanismes innovants pour gérer les carrières des experts en leur permettant de passer de l'un à l'autre et de partager les cultures des deux mondes.

*

**

La société de l'information nous apporte des bénéfices quotidiens. Ses vulnérabilités associées, dont notamment les *APT*, peuvent être vues comme une bonne occasion de repenser nos modes de fonctionnement et de gouvernance. C'est l'occasion pour l'État de structurer une filière qui apporte croissance et sécurité.



■ **Repères - Opinions - Débats**

RDN

Revue Défense Nationale - Juin 2012

Six enseignements stratégiques de l'opération *Unified Protector* de l'Otan en Libye

Florence Gaub

Chercheuse pour le Moyen-Orient au Collège de Défense de l'Otan à Rome. Les vues exprimées ne reflètent pas nécessairement celles du Collège de Défense de l'Organisation du Traité de l'Atlantique Nord.

L'opération *Unified Protector* (*OUP*) fut l'une des missions les plus courtes de l'Otan mais aussi, semble-t-il, l'une des moins controversées. Agissant sous mandat de la Ligue des États arabes et des Nations unies, l'objectif de l'Alliance dans l'*OUP* était de protéger les civils libyens depuis les airs et la mer. Au terme de l'opération, après 204 jours, 26 323 sorties (dont 9 658 sorties offensives) *, 3 124 navires arraisonnés en Méditerranée, le régime du colonel Kadhafi a chuté et de nombreuses pertes civiles ont été probablement évitées. Si l'*OUP* a pu être qualifiée de succès, un bilan équilibré devra toutefois être établi ultérieurement pour prendre en compte l'avenir incertain de la Libye ainsi que l'impact de la crise sur la sécurité régionale.

* SORTIES OFFENSIVES

Les sorties sont généralement des déploiements militaires avec une mission spécifique sans nécessairement impliquer la délivrance d'armes ; les sorties offensives visent à identifier et frapper des cibles déterminées.

Certains commentateurs estiment que, dans le meilleur des cas, l'*OUP* ne peut se targuer d'avoir atteint ses objectifs que par accident, en raison des défaillances que l'opération a révélées dans la structure et les équipements de l'Otan. D'importants enseignements d'ordre technique ont été aussi identifiés dans bien d'autres domaines, tels que le manque de cibleurs et les améliorations à apporter en matière de partage du renseignement ⁽¹⁾. Mais si ces considérations techniques demeurent importantes, il n'en reste pas moins que ce sont d'abord des enseignements stratégiques qui doivent être tirés de l'aventure libyenne de l'Alliance.

Enseignement n° 1 : éviter des conclusions hâtives sur la puissance aérienne

L'*OUP* avait été annoncée comme un conflit « propre », conduit uniquement depuis les airs et la mer, tel que l'avait spécifié la Résolution 1973 du Conseil

de sécurité des Nations unies qui excluait toute « force d'occupation étrangère sous quelque forme que ce soit » ⁽²⁾. Lors de l'opération, l'Otan n'a effectivement déploré aucune victime et sa puissance aérienne a permis de protéger de nombreux civils (la puissance navale y a aussi participé directement mais a été utilisée principalement pour faire appliquer l'embargo sur les armes). On en a alors conclu que l'intervention en Libye préfigurait les conflits de demain, en concrétisant la « tolérance zéro » professée par les pays occidentaux en matière de pertes humaines. Si l'on comprend aisément qu'une telle idée ait pu se répandre, elle n'en reste pas moins erronée.

La faille de ce raisonnement est de laisser croire que le combat des rebelles libyens contre les forces du régime n'a pas été remporté du fait de la supériorité aérienne atlantique alors qu'elle en a bien été un élément décisif. La vraie bataille a été menée au sol par les éléments armés relevant du Conseil national de transition (CNT) de Libye et son important, bien que tenu secret, déploiement de troupes au sol qui ont préféré ignorer la Résolution 1973. À titre d'exemple, on peut citer les troupes envoyées par le Qatar, partenaire de l'Otan dans l'Initiative de coopération d'Istanbul (ICI), mais aussi pour l'*OUP*, qui a reconnu avoir dépêché plusieurs centaines d'hommes pour appuyer les rebelles, en menant des opérations de formation et de communication. Mais surtout, le président du CNT, Mustafa Abdel-Jalil, a déclaré que les batailles décisives qui ont conduit à la victoire ont été préparées par les officiers qataris dans la mesure où les rebelles, pour la plupart des civils sans expérience militaire, étaient incapables d'organiser des forces professionnelles.

Ainsi, alors que l'Otan affirmait ne pas disposer d'une composante terrestre, en fait elle en bénéficiait bien d'une, même si elle n'était pas placée sous son commandement et si l'Alliance ne pouvait pas avoir officiellement de communication directe avec elle. La coordination avec une composante terrestre cruciale ne disposant que d'une formation partielle, placée hors de la structure de commandement et ne pouvant pas être contactée directement, a constitué un défi pour le commandement des forces interarmées de Naples qui a dirigé l'opération. Des solutions créatives ont dû être recherchées pour visualiser la situation sur le terrain et mener la mission au succès. D'après le chef d'état-major du Qatar, le major-général Hamad bin Ali al-Atiya, ce sont leurs officiers de liaison à Naples qui ont assuré la liaison entre l'Otan et les forces rebelles ⁽³⁾.

Dans ce contexte, la guerre « propre » menée ne l'a été que du côté de la force aérienne de l'Alliance. Les forces rebelles, tout comme les civils, ont payé un lourd tribut, bien que le nombre exact de victimes demeure inconnu. Si le ministre de la Santé du CNT a annoncé plus de 30 000 victimes ⁽⁴⁾, on en ignore la répartition entre civils et combattants rebelles. De plus, des violations des droits de l'homme de grande ampleur ont été rapportées par les Nations unies.

L'Alliance elle-même n'a communiqué aucun chiffre mais il est clair que seule une infime partie des victimes est imputable à l'Otan. Ses attaques ont épargné le réseau électrique et les autres infrastructures civiles utiles aux soldats de Kadhafi et, parallèlement, des tracts largués par avion ainsi que des messages radio-diffusés ont demandé aux civils de se tenir à l'écart des infrastructures militaires. *Human Rights Watch* a estimé à environ 50 le nombre de civils tués dans les attaques alliées, tandis qu'une enquête des Nations unies porte ce chiffre à 60 ⁽⁵⁾. Indépendamment des raisons qui ont causé ces pertes, le bilan des morts en Libye n'a pas suscité beaucoup d'échos dans les opinions occidentales qui ont retenu l'image d'un pays peu enclin à critiquer la réussite globale de la rébellion libyenne. Il s'agit là encore d'une conclusion erronée : la puissance aérienne est plus efficace lorsqu'elle est intégrée aux forces armées et les conflits ne peuvent être remportés uniquement depuis les airs ⁽⁶⁾.

Enseignement n° 2 : structure du *Joint Force Command Naples*

Le commandement des forces alliées interarmées de Naples (*JFC Naples*), l'un des trois commandements opérationnels dont dispose actuellement l'Otan, avait reçu pour mission de coordonner les actions militaires nécessaires à la mise en œuvre de la Résolution 1973, en appelant à la protection des civils par tous les moyens nécessaires. Son quartier général, basé dans le Sud de l'Italie, n'a pas de sphère de responsabilité permanente contrairement à son prédécesseur, l'*AFSOUTH* (Forces alliées du Sud Europe). En d'autres termes, sa proximité avec la Méditerranée n'implique pas nécessairement une attention stratégique particulière vis-à-vis de cette région. Lorsque le *JFC Naples* a succédé à l'*AFSOUTH* en 2004, sa mission première escomptée était de fournir une structure allégée et plus flexible, consacrée à diverses opérations telles que le maintien de la paix et l'imposition de la paix sans discrimination géographique particulière. Avant l'émergence de la crise libyenne, le *JFC Naples* dirigeait déjà la mission de formation de l'Otan en Iraq, la Force du Kosovo et l'opération *Active Endeavour* en Méditerranée. Dans ce contexte, sa capacité à diriger l'*OUP* était loin d'être acquise. L'*OUP* avait besoin d'une action cinétique plutôt que d'une opération d'imposition de la paix, et la région concernée exigeait une expertise approfondie.

La rapidité avec laquelle la mission a été décidée, a amené l'Otan à dépêcher à Naples des experts d'autres structures, tandis que le quartier général opérationnel était installé à la hâte dans une salle de danse. Bien qu'il soit possible en théorie de faire appel au Commandement de l'Otan basé à Madrid pour fournir le personnel nécessaire, la rapidité de déclenchement de la mission et les compétences spécifiques recherchées ont exclu cette possibilité. Alors que les lenteurs bureaucratiques de l'Alliance ont semblé parfois ignorer l'urgence de l'action militaire (des officiers des pays partenaires se sont entendus dire que les ordinateurs ne seraient pas disponibles avant trois mois), le *JFC Naples* n'était pas correctement équipé

pour faire face à une crise de cette dimension, même s'il a fait preuve de grandes capacités d'improvisation.

La réforme de la structure de commandement entreprise par l'Otan permet de corriger en partie ces défaillances et le *JFC Naples* est appelé à devenir un quartier général capable de se déployer dans un théâtre jusqu'au niveau d'une opération interarmées de grande envergure. Néanmoins, avec l'incertitude provoquée par le Printemps arabe, le scénario de l'instabilité et de la violence ne peut être exclu et la Méditerranée demeure une zone de préoccupation où l'Otan pourrait avoir besoin de capacités pour y mener des opérations allant de la *R2P* (Responsabilité de protéger : concept des Nations unies visant à prévenir les génocides, crimes de guerre, crimes contre l'humanité et nettoyages ethniques) jusqu'au maintien de la paix. Un équipement et une dotation en personnel appropriés pour le quartier général seraient la conséquence logique de ce qui précède, tout comme le serait l'attribution d'une sphère de responsabilité géographique spécifique.

Enseignement n° 3 : connaître l'ennemi

Bien que Sun Tzu lui-même ait postulé que la connaissance de l'ennemi constitue un élément décisif pour remporter un conflit, l'Alliance a pris le parti d'ignorer cet adage. Aussi surprenant que cela puisse paraître, l'*OUP* n'a engagé aucun conseiller originaire de Libye, ni d'aucun autre pays proche, pour travailler sur cette question. Certains officiers des pays arabes partenaires en poste dans le quartier général opérationnel étaient parfois sollicités pour fournir des conseils mais aucune approche structurée n'était disponible sur un pays qui n'a été que trop peu visité et étudié ces quarante dernières années. La pertinence des hypothèses et prévisions sur le comportement libyen a été bien en deçà des appréciations judicieuses qu'auraient pu formuler des spécialistes de la Libye et de sa culture. Afin de pallier au manque d'expertise permettant de comprendre certains événements survenus dans le pays pendant le soulèvement (par exemple, la difficulté à interpréter l'apparente passivité de la population de Tripoli), il a été fait appel aux connaissances *ad hoc* disponibles sur « les questions arabes ». Lorsque l'Otan a essayé d'anticiper les choix stratégiques des tribus berbères dans l'Ouest du pays, par exemple, elle n'a pas jugé opportun de s'enquérir de conseils avisés. Dans la mesure où la composante terrestre était un élément essentiel de la réussite de la mission, un éclairage culturel aurait été d'une grande utilité pour avoir une compréhension globale de la situation dans le pays au fur et à mesure que se déroulait l'opération.

Comme l'a admis *a posteriori* le *JFC Naples* et on pouvait s'en douter, la Libye présente de grandes différences culturelles par rapport aux pays du Golfe qui ont participé à l'opération. Plus important encore, une connaissance historique et politique de la Libye aurait permis de faciliter la planification stratégique dans une *terra incognita* qui était appréhendée depuis les airs. Compte tenu de la confusion sur les éventuels comportements des différentes tribus, des Berbères et des forces

de Kadhafi, on peut s'interroger sur les raisons du peu d'intérêt porté à la composante culturelle, surtout lorsque l'on sait que toute communication directe avec les rebelles était interdite. Bien qu'elle continue de travailler avec des cultures et des pays très différents de ceux d'Europe ou d'Amérique du Nord, l'Otan manifeste une certaine lenteur à reconnaître l'importance de bien saisir la réalité locale indépendamment de l'aspect purement militaire. La victoire à laquelle l'OUP est finalement parvenue ne doit pas permettre de conclure à l'inutilité des conseillers culturels. La question fondamentale est de savoir si une compréhension approfondie de la réalité locale aurait permis de remporter ce même succès plus tôt, en anticipant, par exemple, le comportement des rebelles et des civils, que ce soit à Tripoli ou à Misrata, sur la base de jugements avisés plutôt que de spéculations.

Enseignement n° 4 : réduire la fracture politico-militaire

Comme l'ont clairement explicité les interprétations juridiques de la Résolution 1973, l'OUP n'a pas cherché à renverser le régime du colonel Kadhafi, ni *a fortiori* à assassiner ce dernier. Malheureusement, le décalage entre les actions militaires et les orientations politiques est apparu au grand jour lorsque les ministres des Affaires étrangères des pays de l'Alliance et les pays partenaires de l'OUP ont appuyé « avec force » l'appel lancé à Kadhafi par le Groupe de contact pour qu'il quitte le pouvoir ⁽⁷⁾. Cela a renforcé l'impression selon laquelle l'opération de l'Otan était réellement sur le point de modifier le régime libyen, indépendamment du fait que le *JFC Naples* continuait à interpréter la Résolution 1973 au sens strict de la protection des populations civiles.

Alors que la pression s'est accentuée au cours de l'été 2011, le général Charles Bouchard, commandant de l'OUP, a dû expliquer que ses ordres « n'étaient pas de procéder à un changement de régime ou de tuer un chef d'État » ⁽⁸⁾. Néanmoins, le net décalage politico-militaire, tout comme celui entre l'Otan en tant qu'ensemble global et ses États-membres pris séparément, a largement contribué à troubler les esprits. Cela a été particulièrement vrai pour la Russie et la Chine, qui avaient validé la Résolution 1973 précisément parce qu'elle ne préconisait pas de changement de régime. Comme l'a montré quelques mois plus tard le cas syrien, le capital politique a été dilapidé par les incohérences relevées au niveau politico-militaire.

Il y a eu un déplacement du problème politique vers la sphère militaire, dans laquelle il n'avait rien à faire, et le bras armé de l'Otan s'est retrouvé confronté à un véritable casse-tête.

Il en a été de même en ce qui concerne la distinction juridique entre les restrictions des Alliés et les restrictions nationales. N'étant pas autorisé à avoir des contacts directs avec les rebelles, le général Bouchard a rencontré le chef du CNT au titre de sa citoyenneté canadienne. Le rôle du Qatar, partenaire de l'Otan participant à l'OUP qui a délibérément outrepassé la Résolution 1973 en envoyant des forces terrestres en Libye, a déjà été mentionné plus haut ⁽³⁾. Dans l'esprit du public,

cette distinction juridique n'est pas évidente et entretient une confusion entre l'Otan en tant qu'ensemble et ses membres individuels ou nations partenaires.

Enseignement n° 5 : améliorer la communication stratégique

Malgré les efforts considérables déployés par l'Otan pour expliquer son action en Libye avec la création de chaînes sur *YouTube* et la tenue de conférences de presse quotidiennes, sa production médiatique est demeurée plutôt modeste comparée à celle du régime Kadhafi réalisée avec l'aide d'une entreprise de relations publiques. L'Otan ne pouvait tout simplement pas rivaliser avec la *BBC*, qui avait accès aux hôpitaux et à qui on montrait des cadavres de jeunes enfants, ou même recourir à la rhétorique traditionnelle arabe utilisant des termes comme « colonialisme » ou « impérialisme ». Si l'Otan a refusé de se prononcer clairement sur le nombre de pertes civiles, les médias arabes et russes ont avancé des chiffres bien supérieurs à 1 000 en ce qui concerne le nombre de civils tués ou blessés par les frappes aériennes de l'Alliance ⁽⁹⁾.

Malgré le soutien de l'opinion arabe à l'opération de l'Otan, la couverture médiatique a adopté un ton neutre ou négatif selon les régions et est demeurée instable tout au long du conflit. *Al-Jazeera*, chaîne avec laquelle l'Alliance s'était déjà brouillée dans le passé sur l'Afghanistan, a nettement défendu l'opération et contribué à renforcer le soutien de l'opinion arabe mais d'autres médias se sont montrés plus critiques en dénonçant les pertes civiles. Par conséquent, l'image traditionnellement négative de l'Otan dans la région est demeurée inchangée. L'impact à long terme de l'OUP à cet égard dépendra en grande partie de l'évolution de la situation interne en Libye. Bien que la contribution de l'Alliance ait très vraisemblablement permis d'épargner un grand nombre de civils, le rôle qu'elle a joué dans ce domaine pourrait bien être assombri par de futures évolutions négatives.

Dans l'ensemble, la communication stratégique des forces du régime (ainsi que celle du Conseil national de transition) a été plus sensible au sentiment local du public cible et donc au profil médiatique le plus pertinent. Par ailleurs, la création extrêmement rapide de la chaîne de télévision rebelle *Libya Ahrar* (Libye libre) témoigne d'une agilité et d'une adaptabilité toujours plus fortes en matière de communication stratégique. L'Otan doit en tirer les leçons qui s'imposent et s'adapter à ce nouveau contexte le plus vite possible.

Enseignement n° 6 : absence de vision stratégique pour la région

L'abstention de l'Allemagne lors du vote de la Résolution 1973 au Conseil de sécurité des Nations unies a été largement perçue comme une rupture de la cohésion de l'Alliance, tout comme l'a été la participation limitée des Alliés dans l'opération. Cela n'a été que la conséquence logique du manque de vision commune pour la région du Moyen-Orient et de l'Afrique du Nord qui n'a cessé de miner

l'Otan depuis sa création : les conflits de la région, à l'exception peut-être de l'Irak en 1991, ont toujours divisé les Alliés.

Malgré les deux programmes de partenariat de l'Alliance, le Dialogue méditerranéen et l'Initiative de coopération d'Istanbul, les membres de l'Otan entretiennent encore aujourd'hui des différences de point de vue substantielles sur la façon d'appréhender cette région. Cela ne s'explique pas uniquement par l'héritage des quarante premières années de l'Alliance, lorsque la Méditerranée et sa rive Sud étaient pratiquement confinées par le contexte de la guerre froide. C'est aussi le fruit d'analyses divergentes sur les régions présentant le plus d'intérêt pour l'Alliance après la fin de la menace soviétique. En fonction de leur situation géographique respective, les Alliés ont tour à tour désigné le Centre, le Nord ou le Sud.

Ce manque de vision reflète avant tout une forte préférence des pays alliés pour une approche bilatérale ou trilatérale lorsqu'ils traitent avec cette partie du monde. Compte tenu de l'enjeu international qu'elle représente du fait de ses ressources pétrolières, de sa route commerciale Ouest-Est vitale et de ses points de passage obligés susceptibles de paralyser une grande partie du commerce mondial, la région suscite la convoitise d'Alliés dont les intérêts stratégiques pourraient menacer le consensus de l'Otan. Par conséquent, l'Alliance doit s'accorder sur une vision commune si elle souhaite conserver son influence chez ses voisins du Sud.

*
**

L'euphorie suscitée par la chute d'un régime brutal qui a duré quatre décennies en Libye ne doit pas masquer le fait que les conséquences de l'OUP ne sont pas encore totalement observables. En effet, d'autres enseignements sont susceptibles de surgir plusieurs années après la fin de l'opération. Ce serait une erreur de penser que l'aventure de l'Otan en Libye s'est achevée avec la fin de la mission militaire. Que cela plaise ou non à l'Alliance, sa réputation est en jeu dans le long processus de reconstruction de la Libye.

ÉLÉMENTS DE BIBLIOGRAPHIE

- (1) *RUSI, Accidental Heroes: Britain, France and the Libya Operation*, septembre 2011 (www.rusi.org/).
- (2) Résolution 1973 du Conseil de sécurité des Nations unies, 17 mars 2011 (<http://daccess-dds-ny.un.org/doc/>).
- (3) *Al-Arabiya, Qatar admits it had boots on the grounds in Libya; NTC seeks further NATO help*, 26 octobre 2011 (www.alarabiya.net/).
- (4) *Tripoli Post, At least 30,000 Killed, 50,000 Wounded in Libyan Conflict*, 8 septembre 2011 (www.tripolipost.com/).
- (5) *Al Arabiya News, HRW urges NATO to probe Libyan civilians' deaths but Libya says no need to investigate*, 16 décembre 2011 (www.alarabiya.net/) ; Conseil des droits de l'homme des Nations unies, Rapport de la Commission d'enquête internationale sur la Libye, New York, 2 mars 2012.
- (6) Grant T. Hammond, *Myths of the Air War over Serbia: Some 'Lessons' Not to Learn*, *Aerospace Power Journal*, hiver 2000 (www.airpower.au.af.mil/).
- (7) Otan, Déclaration sur la Libye, 14 avril 2011 (www.nato.int/).
- (8) *BBC News, Libya conflict: NATO's man against Gaddafi*, 26 juin 2011 (www.bbc.co.uk/).
- (9) *Russia Today, Civilian cost of NATO victory in Libya*, 20 octobre 2011 (<http://rt.com/news/>).

Mali : vive la Coloniale !

Claude Le Borgne | Général (CR).

Les empires ont du bon. Leur mérite est de maintenir en paix, sous leur rude férule, des peuples belliqueux. L'empire austro-hongrois et l'empire ottoman en sont deux beaux exemples. L'un et l'autre n'ont pas survécu à la Grande Guerre. On connaît la suite, en Yougoslavie pour le premier, un peu partout dans les Orientes pour le deuxième. Il en est un troisième, dont un anticolonialisme primaire empêche qu'on reconnaisse les bienfaits, l'empire africain de la France. Sans doute la décolonisation douce – sauf en Algérie – qui a présidé à son démembrement a-t-elle longtemps occulté ce que celui-ci recelait de braises sous la cendre : populations diverses, dialectes innombrables, frontières tracées au cordeau au mitan de tribus homogènes, pasteurs et agriculteurs, nomades et sédentaires, Noirs et Blancs, animistes, chrétiens et musulmans. La paix surprenante qui, bon an mal an, a régné sur notre empire défunt est-elle en passe d'être rompue ? Les récents incidents au Mali incitent à le redouter. Voyons voir !

Le Sahel sud-saharien, zone de transition entre savane et grand désert, qui court du rivage atlantique au centre de l'Afrique à travers Mauritanie, Mali, Niger et Tchad, est particulièrement exposé aux troubles attendus. L'ensemble est partagé entre trois ethnies de culture nomade : les Maures à l'Ouest, formidables guerriers arabo-berbères * que nous eûmes bien du mal à rallier à notre cause, ce qui ne fut accompli qu'en 1934 ; les Touareg (*dans l'indécision où nous place l'écriture de ce mot curieusement arabe, nous écrirons Touareg au pluriel et Targui au singulier*) au centre, berbères bon teint dont les talents de dresseurs de chameaux, les coutumes originales, la tiédeur musulmane et le motif cruciforme de leur artisanat ont nourri un temps les illusions du Père de Foucault et leur ont permis de voler aux Maures le vedettariat médiatique ; à l'Est enfin, les Toubous, dont l'ascétisme bédouin vaut, paraît-il, celui des Maures.

* LES MAURES

Les Maures donnent, dans la conjoncture actuelle, une nouvelle preuve de leurs qualités multiples : l'armée mauritanienne est la plus active et la plus efficace dans la lutte contre AQMI, d'autres isolés combattent dans les rangs des islamistes et le gouvernement mauritanien est sollicité pour la solution d'un problème qui ne le concerne qu'à demi.

Des troubles annoncés, la Mauritanie s'est bien sortie et il convient de rendre hommage à l'œuvre de son premier président, Mokhtar ould Daddah, réussissant à faire cohabiter Bidhanes (« hommes blancs » ainsi qu'ils se nomment) et Noirs alors qu'historiquement les premiers dominaient les seconds sans partage.

Certes, le torchon a brûlé entre ces deux « couleurs » et, par contrecoup, entre Maures et Sénégalais, en avril 1989. Mais c'est dans le Nord du pays, ex-colonie espagnole, qu'une tentative sécessionniste s'est concrétisée ; le problème créé, bien malencontreusement, par le Front Polisario (acronyme significatif de son origine coloniale : Front pour la Libération du Sahara espagnol et du Rio del Oro) dès l'année 1973 n'est toujours pas résolu.

Ayant mis, non sans raisons, la Mauritanie à part, laissons les Toubous dans leur Nord tchadien, n'oubliant pas, pourtant, que c'est la cohabitation des Toubous, que l'on peut, grossièrement, qualifier de Blancs, et des Noirs du Sud qui nous ont entraînés à revenir à plusieurs reprises donner la main à des gouvernants débordés par ce redoutable clivage. Limitons-nous maintenant aux prestigieux Touareg.



Élargissons pourtant le paysage, illustration de ce que nous disions des découpages coloniaux. S'il y a un bon paquet de Touareg au Mali, il y en a un aussi gros au Niger, un petit en Algérie mais très célébré, un reliquat en Libye. Au Mali, ils nomadisaient – l'imparfait s'impose – dans le Nord-Est du pays, soit, vite dit, l'Azaouad où les massifs montagneux de l'Adrar des Iforas et du Timétrine atténuent la rigueur du climat saharien, comme d'autres le font au Niger (Aïr), en Algérie (Hoggar), au Tchad (Tibesti-Ennedi). Mais les aléas climatiques, l'attrait du modernisme, l'action des gouvernants, ont amené nombre de nomades maliens à migrer vers le Sud et à s'y sédentariser. Il convient de rappeler ici que les nomades sont, pour les États, des gêneurs. En toute bonne conscience, les gouvernements souhaitent que leurs nomades profitent de leurs services, éducation, santé et... fiscalité. De la Mauritanie à la Somalie. Le phénomène est général. En Mauritanie, il est particulièrement visible mais partout les civilisations nomades sont en train de mourir. Il n'y aura bientôt plus que quelques vieux méharistes de chez nous pour regretter cette merveille culturelle qu'était l'exploitation du vide. Pourtant, les militants irrédentistes utilisent sans vergogne un prestige qu'ils ne méritent plus. Ainsi, de longue date, ceux du Front Polisario et, maintenant, ceux de l'Azaouad font-ils miroiter aux yeux des gogos d'Occident le modèle de l'État nomade, monstre jamais vu et désormais mythique.

C'est ce mythe qu'utilise, apparemment, le MNLA, Mouvement national de libération de l'Azaouad, négligeant, par sa dénomination même, le nombre supérieur de Touareg qui, plus ou moins sédentarisés, résident hors Azaouad dans le Sud du Mali et, bien sûr, le nombre encore plus grand de leurs frères sahariens extérieurs. Certes, la cause irrédentiste au Mali et au Niger est une vieille affaire, maîtrisée non sans mal par les gouvernements successifs des deux pays. Elle a pris un tour nouveau. La liquidation en Libye du régime de Kadhafi n'a pas encore dévoilé toutes ses conséquences et les premières qui soient visibles ne sont pas encourageantes. Les Touareg aiment bien la guerre. Quelques-uns s'étaient mis au service du « berger des Syrtes »⁽¹⁾. Le berger disparu, ces mercenaires au chômage regagnent leur pays, convoyant au retour des stocks d'armes et de munitions.

Le Président nigérien a habilement négocié avec ses revenants. Le gouvernement de Bamako, que présidait Amadou Toumani Touré, dit ATT, en fin de mandat, n'a pas pris la même voie. Il est vrai qu'il n'en pouvait mais : pour venir à bout de sa pauvre armée, ses Touareg à lui ont reçu le soutien d'alliés encombrants mais efficaces, les islamistes d'AQMI, Al-Qaïda au Maghreb islamiste. Le GSPC algérien, Groupe salafiste pour la prédication et le combat, est l'ancêtre d'AQMI. Le premier intitulé proclamait de façon agressive une option radicale. Le second plaçait le mouvement sous la bannière, alors flatteuse, d'Oussama ben Laden. Le GSPC/AQMI s'en prit d'abord à l'Algérie. En résulta l'affreuse guerre civile qui y fit quelque 150 000 morts en dix ans. La coûteuse victoire du pouvoir algérien obligea AQMI à abandonner ce théâtre initial et à se réfugier au désert. Depuis lors, le mouvement mariant techniques modernes et pratiques sahariennes ancestrales (mariage qu'a

tenté de décrire Jean-Christophe Rufin dans son roman *Katiba* ⁽²⁾, s'est spécialisé dans le fructueux commerce des otages. Ce *business* fut inauguré en 2003, de façon spectaculaire, par l'enlèvement de 32 touristes allemands, libérés contre 5 millions de dollars payés par... la Fondation Kadhafi pour les actions humanitaires ⁽³⁾. Rappelons que les otages enlevés à Arlit au Niger dans le complexe d'Areva le 16 septembre 2010 sont toujours détenus par AQMI et probablement dans le massif du Timétrine, au Mali, nous y revoilà.

MNLA targui et AQMI islamiste semblent avoir fait cause commune. L'alliance est pourtant contre nature, vice que camoufle la création d'une branche malienne d'AQMI, baptisée *Ansar ed Dine* et placée aux ordres d'un *Iyad ag Ghali*, dont le patronyme atteste la « targuitude ». Le camouflage ne peut tromper personne : le 4 mai dernier à Tombouctou, les activistes d'*Ansar ed Dine* ont profané la tombe d'un saint « marabout ». Ainsi le mouvement s'inscrit-il clairement dans la pure orthodoxie, musulmane et wahhabite, pour laquelle le culte des saints et l'islam confrérique, si développés en Afrique, sont un scandale.

Quelle que soit la fragilité de l'alliance MNLA/AQMI, son succès initial était prévisible face à une armée malienne misérable. L'Azaouad est aux mains du MNLA en janvier 2012 et AQMI, sur le fleuve Niger, parade à Tombouctou comme, à Gao, Boko Haram. Boko Haram, quoi encore ? « Occidentalisation interdite », sous ce drapeau militent les islamistes nigériens – et non nigériens – les plus engagés. Si, en effet, nous avons jusqu'ici opposé Blancs et Noirs, nomades et sédentaires, il faut imaginer une autre frontière plus au sud, entre musulmans et « infidèles », que ceux-ci soient chrétiens ou animistes. Cette frontière-là, au sud du Sahel qui nous occupe ici, partage aussi maints pays – sinon tous – issus de la décolonisation. Ainsi au Burkina Faso, en Côte d'Ivoire, au Bénin, au Togo, au Sénégal même et au Nigeria où la guerre civile s'installe.

Dans ce méli-mélo, le pouvoir de Bamako ne pouvait que s'effondrer. L'armée, soucieuse de sauver son honneur, dénonce l'impéritie d'ATT, responsable de son dénuement et de son impuissance. Le putsch du capitaine Amadou Haya Sanogo dépose le président le 22 mars, à deux mois de la fin programmée de son mandat. Le putsch est, on le sait, la façon africaine de pratiquer l'alternance. Celui-ci paraissait bénin, le capitaine signant un « accord-cadre » qui permet l'établissement d'un pouvoir intérimaire présidé par Diacoundé Traoré, secondé d'un Premier ministre décoiffant : Cheikh Modibo Diarra possède la nationalité américaine et une réputation internationale d'astrophysicien. On croyait l'affaire réglée et ATT aux oubliettes. Pas du tout ! Le 30 avril, sa garde parachutiste, apparemment fidèle, déclenche un contre putsch pour éliminer la junte de Sanogo, toujours là, mais échoue au prix de quelque 14 morts et 40 blessés.

L'affaire en étant à ce point, toute prévision serait imprudente. À Bamako le pouvoir balance, au moment où nous écrivons, entre Sanogo, Traoré, ATT. L'armée, que l'on pensait unie pour recouvrer son honneur perdu, est divisée. Dans

le Nord, les deux protagonistes ont des vues opposées. Il se peut que le MNLA, maître d'un Azaouad dont l'indépendance est invivable, négocie un statut nouveau pour cette province saharienne. AQMI a des ambitions plus vastes et plus dangereuses, servies – ou concurrencées – par celles de Boko Haram : voici, une fois de plus, l'islam au pied du mur.

Souhaitons bonne chance à la Cédéao, Communauté des États d'Afrique de l'Ouest, inévitable médiateur, et espérons que la sagesse de nos propres dirigeants les gardera de mettre le doigt dans ce chaudron de sorcière.

ÉLÉMENTS DE BIBLIOGRAPHIE

- (1) Guy Georgi : *Kadhafi, le berger des Syrtes* ; Flammarion, 1998.
- (2) Jean-Christophe Rufin : *Katiba* ; Flammarion, 2010.
- (3) Atmane Tazaghart : *AQMI - Enquête sur les héritiers de Ben Laden au Maghreb et en Europe* ; Éditions Picollec, 2011.

Le dilemme syrien du *Hezbollah*

Jean-Loup Samaan

Maître de conférences, département Moyen-Orient du Collège de défense de l'Otan, docteur en science politique (Université Paris 1). Auteur des *Métamorphoses du Hezbollah* (Éditions Karthala, 2007).

A l'approche du printemps 2011, tout semblait réussir au *Hezbollah* libanais. Ses forces au Sud du Liban s'étaient non seulement réorganisées mais renforcées cinq ans après la guerre contre Israël. À Beyrouth, le nouveau gouvernement de Najib Mikati prenait ses distances avec l'agenda pro-occidental promu par son prédécesseur, Saad Hariri, et relâchait temporairement la pression sur le Parti de Dieu vis-à-vis du Tribunal spécial sur le Liban. Enfin, le mouvement récupérait à ses propres fins les premiers soulèvements en Tunisie, Égypte et Bahreïn. Pour les dirigeants du Parti, le parallèle symbolique entre le Printemps arabe et l'historiographie chiite libanaise était une aubaine : dans les deux cas, il était ainsi question de lutte des opprimés contre les puissants, des laissés-pour-compte contre la minorité dominante. Le cas bahreïni était d'autant plus évident que le petit royaume du Golfe est le théâtre d'une contestation menée par une population majoritairement chiite contre une famille régnante sunnite. Autrement dit, le *Hezbollah* trouvait dans les premières semaines du Printemps arabe une belle occasion de rappeler ses propres origines révolutionnaires.

Cependant, le basculement de la Syrie dans une guerre civile opposant le régime de Bashar al Assad – soutien politique et financier historique du *Hezbollah* – à sa population est venu bousculer la stratégie politique du mouvement libanais et l'a mis face à un dilemme crucial : le *Hezbollah* devait-il soutenir le régime d'Assad afin de préserver une alliance régionale au risque d'éroder son image de force sociale luttant pour les opprimés ?

La dette stratégique du *Hezbollah* envers le régime syrien

Produit de la guerre civile libanaise et de l'invasion israélienne du pays en 1982, le *Hezbollah* est devenu en l'espace de trois décennies la plus puissante organisation non-étatique, politiquement et militairement. Issu de la communauté chiite, le *Hezbollah* a pu s'étendre grâce à ses relations avec deux alliés régionaux qui comptent beaucoup au Liban : l'Iran et la Syrie. À l'origine, le mouvement s'inspire de la révolution iranienne de l'*ayatollah* Khomeiny qu'il souhaite propager au Liban mais à partir des années 1990, après la guerre civile, il se montre plus pragmatique et ce, pour ne pas s'aliéner une partie de la scène politique libanaise.

Son actuel *leader*, Hassan Nasrallah, est l'artisan majeur de ce travail de « libanisation » du mouvement. Âgé de 51 ans, Nasrallah incarne le Parti depuis qu'il en a pris la tête en février 1992, après l'assassinat par les forces israéliennes du précédent secrétaire général, Abbas Moussawi. Orateur charismatique, Nasrallah devient au fil des années une icône dans les pays arabes en tant que figure de proue de la résistance face à Israël. En 2006, ses forces armées réussissent même à infliger à Israël des dommages qu'aucune armée arabe n'avait pu provoquer auparavant ⁽¹⁾. Nasrallah inspire même le respect des planificateurs israéliens qui loin d'en faire un fanatique irrationnel, le décrivent comme un fin stratège politique et militaire.

Durant toutes ces années, cette assise politique et militaire du *Hezbollah* n'a pu être possible que grâce à un mariage de convenance avec le régime syrien qui, depuis son intervention militaire en 1976 au Liban fait et défait les gouvernements à Beyrouth. Hafez al Assad, le père de l'actuel président syrien, n'aimait guère le Parti de Dieu : il regardait avec suspicion non seulement la rhétorique islamique qui ornaît la propagande du mouvement mais aussi les liens entre les Gardiens de la Révolution iraniens et le *Hezbollah*. Bien qu'Hafez al Assad ait fait alliance avec l'Iran de Khomeiny, il entendait clairement signifier à celui-ci et à ses proches que le Liban restait terre d'influence syrienne. C'est pourquoi si Assad autorisa le passage en Syrie des convois iraniens vers le Liban, il maintint une certaine distance avec le *Hezbollah* et de nombreux observateurs affirment qu'il n'aurait rencontré Hassan Nasrallah qu'à deux reprises en quinze ans ⁽²⁾.

La relation entre le *Hezbollah* et la Syrie change substantiellement avec l'arrivée de Bashar al Assad qui prend la tête du pays en juin 2000. Nasrallah devient un visiteur régulier de Damas et le nouveau président syrien n'hésite plus à s'afficher publiquement avec celui-ci. Le régime syrien développe l'idée d'un axe anti-impérialiste représenté par Bashar al Assad, Hassan Nasrallah et, à partir de 2005, Mahmoud Ahmadinejad, le président iranien. La retenue d'Hafez est donc bien dépassée. Signe de cette évolution, à l'été 2006, en pleine guerre entre Israël et le *Hezbollah*, les rues de Damas ou d'Homs sont bardées d'affiches à la gloire du mouvement, et de Nasrallah en particulier.

À ce soutien politique, s'ajoute un appui logistique syrien à la composante militaire du Parti de Dieu. Non seulement Bashar al Assad maintient les voies syriennes d'approvisionnement des armes iraniennes vers le *Hezbollah* mais il facilite l'accès du mouvement à des technologies de pointe. La Syrie aurait transféré en avril 2010 des missiles balistiques *Scud-D* au *Hezbollah* (allonge estimée à 700 km, en portée de Jérusalem ou Tel Aviv) ⁽³⁾. Ce transfert fait suite à une première suite d'allégations sur la fourniture au *Hezbollah* par Damas de missiles *M-600*, une variante du *Fateh-110*, pouvant frapper jusqu'à 300 kilomètres.

Début 2012, le nombre de roquettes dont disposerait le *Hezbollah* est incertain. On estime aujourd'hui l'arsenal du mouvement à environ 42 000 roquettes auxquelles s'ajouteraient 4 000 missiles de courte ou moyenne portée. En tous les

cas, si la force de frappe du Parti de Dieu constitue aujourd'hui non plus une simple capacité de nuisance sur le Nord d'Israël mais un véritable outil de dissuasion à l'égard de l'État hébreu, c'est bien grâce à l'aide du régime syrien de Bashar al Assad.

Un soutien indéfectible du *Hezbollah* à Bashar al Assad ?

À plusieurs reprises au cours de la dernière décennie, le *Hezbollah* a pris le risque de perdre son assise populaire en soutenant Bashar al Assad. Déjà en 2005, l'assassinat de Rafic Hariri, ancien Premier ministre libanais, devenu opposant à la présence syrienne au Liban déclencha une vague de protestations contre Damas. Les manifestations se soldèrent par le départ des troupes syriennes et l'arrivée d'un gouvernement issu de l'alliance politique antisyrilienne. Tout au long de ces événements, Hassan Nasrallah n'hésita pas à clamer son soutien indéfectible à Bashar al Assad et le *Hezbollah* supervisa de multiples contre-manifestations à Beyrouth et ce, au risque de se voir accuser d'aller à l'encontre des intérêts nationaux libanais. Le mouvement a semblé alors pris dans un jeu d'équilibriste pouvant se retourner fatalement contre lui et seule la guerre contre Israël, l'été suivant, lui a permis de surmonter les divisions internes libanaises pour faire front contre Tsahal.

Or, aujourd'hui, plus qu'en 2005, la stratégie de « libanisation » du *Hezbollah* se trouve dans une impasse. Pendant les premiers mois qui ont suivi la crise syrienne, Nasrallah et ses proches conseillers ont conservé la même posture que lors des précédentes vagues contre le régime syrien en lui offrant un soutien indéfectible. Jusqu'à mars 2012, les quelques discours prononcés par le secrétaire général du Parti de Dieu sur la Syrie adoptent une même structure rhétorique : la dénonciation des stratégies prédatrices des puissances extérieures (États-Unis, Israël) contre le régime syrien et le rappel de la cause palestinienne jugée plus urgente. En d'autres termes, le mouvement développe un narratif de la crise identique à celui du gouvernement de Bashar al Assad. Si certains médias, notamment en Israël, évoquent un soutien logistique du *Hezbollah* dans la répression syrienne, le mouvement nie toute implication.

Mais contrairement aux attentes du *Hezbollah*, la crise syrienne ne s'est pas résorbée et s'est au contraire transformée progressivement en guerre civile. À partir de février 2012, l'offensive des forces syriennes sur Homs suscite une émotion internationale. De plus en plus de protestations dénoncent le soutien du *Hezbollah* et des vidéos circulent sur *Internet* montrant des Syriens accusant nommément Nasrallah ou brûlant le drapeau du *Hezbollah*.

Le 15 mars marque un tournant. Alors qu'Hassan Nasrallah prononce un discours public sur le système éducatif libanais, il en vient, au bout d'une dizaine de minutes, à la question syrienne et appelle, pour la première fois, les deux parties à prendre le chemin de la résolution pacifique de leurs contentieux. En d'autres termes, il place désormais sur le même plan le régime et ses opposants. Nasrallah

ajoute que le gouvernement à Damas doit faire la lumière sur les mois d'affrontements et offrir la vérité à sa population. Si certains observateurs se sont trop vite empressés d'y voir un lâchage d'Assad par Nasrallah, ce discours signale *a minima* la prise de conscience du *leader* libanais des limites de son soutien ⁽⁴⁾.

Par conséquent, le *Hezbollah* est aujourd'hui dans une situation critique : maintenir son appui à Assad, alors que la fin de son régime est désormais envisageable, peut lui aliéner une majorité de Libanais mais aussi les éventuels successeurs du régime à Damas. La position tenue par Nasrallah mi-mars, et répétée quelques semaines plus tard lors d'un entretien avec Julian Assange pour la télévision russe, tente de concilier son soutien au régime et la reconnaissance des légitimes protestations. Ce changement rhétorique pourrait néanmoins arriver trop tard pour permettre au *Hezbollah* de sortir intact de la crise syrienne, qui plus est avec le risque grandissant d'extension de celle-ci au Liban.

Le Hezbollah sans le régime d'Assad

Si un changement de régime à Damas entraînerait des répercussions sur l'ensemble du Moyen-Orient, à commencer par le Liban, il ne faut pas se laisser abuser par l'image d'un effet domino qui verrait rapidement le *Hezbollah* s'effondrer. Si le règne de Bashar al Assad venait à s'achever, les voies syriennes d'approvisionnement entre l'Iran et le Parti de Dieu seraient vraisemblablement affectées. En effet, plusieurs figures de l'opposition syrienne, telles que Burhan Ghalioun, ont fait savoir que l'alliance Damas-Téhéran ferait l'objet d'un ré-examen. Un réalignement de la Syrie post-Assad couperait donc l'accès stratégique de l'Iran au Moyen-Orient et pourrait affecter également le *Hezbollah* qui perdrait un allié sur lequel compter, non seulement militairement vis-à-vis d'Israël mais politiquement à Beyrouth vis-à-vis de ses opposants. Il y a fort à parier que le *Hezbollah* serait alors en position de faiblesse quant à la mise en accusation de ses membres par le Tribunal spécial pour le Liban. Et on a bien du mal à imaginer que le gouvernement de Najib Mikati – produit des rapports de force entre *Hezbollah*, le Courant patriotique libre de Michel Aoun d'un côté et les courants anti-syriens de l'autre – puisse survivre à moyen terme à un tel changement régional.

Pour autant, un nouveau régime syrien ne priverait pas le *Hezbollah* de ses capacités militaires. Selon toute vraisemblance, le Parti de Dieu dispose encore aujourd'hui d'un arsenal déployé dans le Sud du Liban bien suffisant pour tenir tête à Israël ou à quelques rivaux libanais que ce soient. De plus, selon les autorités militaires israéliennes, le mouvement aurait également été entraîné militairement par des conseillers syriens pour la défense antiaérienne, lui permettant de se prémunir contre d'éventuelles frappes d'Israël ⁽⁵⁾.

Néanmoins, en l'absence de nouvelles voies d'approvisionnement entre l'Iran et le *Hezbollah* – les routes maritimes étant trop exposées à une attaque israélienne – ce rapport de force pourrait se dégrader et susciter des tentations des

opposants extérieurs et intérieurs au *Hezbollah*. Les forces israéliennes pourraient, par exemple, être tentées de conduire une opération de décapitation du mouvement, en ciblant ses infrastructures au Sud et son quartier général en banlieue de Beyrouth. Le *Hezbollah* pourrait alors réagir par une escalade verticale du conflit (lancement de roquettes voire de missiles de courte portée sur Tel Aviv et Jérusalem) et par un effet de mobilisation horizontale (appel à un front simultané dans la bande de Gaza et en Cisjordanie). Ce scénario reste pour l'heure peu probable, Israël ayant adopté une approche prudente depuis le déclenchement des événements en Syrie.

*
**

Il n'en reste pas moins que les mois qui viennent seront décisifs pour la survie du *Hezbollah*. Compte tenu de l'intensité de la crise syrienne, le mouvement ne peut plus revenir en arrière et ce, malgré les subtiles évolutions rhétoriques de Nasrallah. Qu'Assad reste ou pas à Damas n'est plus la question centrale : dans les deux cas, le *Hezbollah* devra faire avec un solide allié régional en moins. Demain, le véritable enjeu pour le mouvement sera de préserver ce qui reste de la longue entreprise de libanisation poursuivie tout au long des années 1990 par Nasrallah et mise à mal la décennie suivante par les crises politiques successives de 2005, 2008 et celle qui est en cours. C'est ainsi moins des capacités militaires du Parti – encore bien suffisantes pour se maintenir face à Israël – que de sa base politique que pourrait découler sa perte.

ÉLÉMENTS DE BIBLIOGRAPHIE

- (1) Travaux de Stephen Biddle, Jeffrey Friedman : *The 2006 Lebanon Campaign and The Future of Warfare: Implications for Army and Defense Policy*, Washington, *Strategic Studies Institute*, 2008 ; Avi Kober : "The Israel Defense Forces in the Second Lebanon War: Why the Poor Performance ?", *Journal of Strategic Studies*, Vol. 31, n° 1, février 2008.
- (2) Nicholas Blanford : *Warriors of God: Inside Hezbollah's Thirty Year Struggle Against Israel*, New York, *Random House*, 2011 ; Emile El-Hokayem : "Hezbollah and Syria: Outgrowing the Proxy Relationship", *Washington Quarterly*, printemps 2007.
- (3) Charles Levinson, Jay Solomon : "Syria Gave Scuds to Hezbollah, US Says", *Wall Street Journal*, 14 avril 2010.
- (4) Nicholas Noe : "Hezbollah's subtle shift on Syria", *Middle East Channel*, blog de *Foreign Policy*, 30 mars 2012. (http://mideast.foreignpolicy.com/posts/2012/03/30/hezbollahs_subtle_shift_on_syria).
- (5) Gili Cohen : "Syria training Hezbollah to use anti-aircraft guns", *Haaretz*, 18 mars 2012.

Le Printemps arabe à l'épreuve du salafisme

Khalifa Chater | Professeur en histoire contemporaine (Université Tunis-1), chroniqueur à la *Revue Défense Nationale*.

L'accès au pouvoir des partis islamistes dans les pays du Printemps arabe (Égypte, Tunisie, Yémen) a été accompagné par l'émergence d'un mouvement salafite qui s'érige désormais en acteur sur la scène politique. Bien longtemps, la mouvance salafite a accordé la priorité à la prédication et s'est accommodée d'une reconnaissance plus ou moins assumée des régimes en place, les ménageant par son éthique du respect des autorités ou par crainte d'un affrontement dans des rapports de forces inégales.

Les courants djihadistes qui s'étaient démarqués et ont opté pour la résistance armée ont été sérieusement mis à l'épreuve et réprimés. Ce qui explique leur passage à la clandestinité. Les « révolutions » du Printemps arabe et la libération de leurs cadres emprisonnés accordent en conséquence aux salafites une plus grande marge de manœuvre. Ils s'adaptent au nouveau contexte et dépassent volontiers leur stratégie piétiste. Tout en faisant partie de la même famille politique que les Frères musulmans, des courants salafites participent à la lutte pour la conquête du pouvoir et forment des partis. Ils ont entre eux des rapports complexes de complicité, de concurrence et d'affrontement.

Définitions et discours fondateur

L'historiographie arabe désigne « le *salaf es-salah* » (les prédécesseurs pieux, de bonne conduite) comme modèle de bon comportement musulman. Le Prophète et ses compagnons, principalement les premiers califes, représentaient l'idéaltype qu'on invite les fidèles à suivre. Cette référence historique est désormais transgressée, puisque le salafisme désigne un mouvement islamiste spécifique. Le retour à « l'Islam des origines » impliquait pour les salafites une lecture littérale du texte sacré. Cette restriction-perturbation du concept originel définit désormais la mouvance et la distingue de la pratique de l'Islam en vigueur dans les écoles sunnites, chiïtes et kharijites. Privilégiant, parmi les penseurs arabes, Ibn Taymiya et Mohamed ibn Abdelwahab, ils les adoptent comme leurs références idéologiques.

Considérant le modèle des anciens, les *salaf*, comme un absolu, Ibn Taymiya (1263-1328) s'appuie uniquement sur le Coran et sur le *hadith*. Il dénonce, dans ce cadre, tout ce qu'il juge innovation (*bidaa*) en Islam et attaque les partisans

du soufisme. Il inspira Mohamed ibn Abdelwahab (1703-1792) qui établit les règles du *tawhid* (*praxis* du monothéisme), condamnant le culte des saints et interdisant la pratique de leur intercession (*tawassoul*), le considérant comme de l'idolâtrie. Dans les deux cas, la lecture littérale des références relativise et réduit le rôle du consensus (*ijma*) et limite le champ de l'*ijtihad*, principes fondés sur des jugements de valeur trop humains, selon ces théologiens.

Faisant partie de la mouvance de l'Islam politique, le mouvement salafite diffère, selon ses courants, du mouvement des Frères musulmans, par son rejet absolu de la démocratie et de la souveraineté populaire, comme « innovations », non compatibles avec le respect de la volonté de Dieu. « La démocratie est un danger puisqu'elle confie la référence de la législation au peuple » affirma le prédicateur égyptien Abdel Moumen Ech-Chaat. Il s'oppose, d'autre part, à la participation au Parlement des femmes et des juifs. D'autre part, il prône le régime du califat, pour réaliser l'unité de l'*oumma*, la communauté musulmane ⁽¹⁾.

Attitude similaire du parti salafite tunisien, *Hizb at-Tahrir*, qui prône le califat comme régime politique, se déclare antidémocratique et adopte comme références exclusives le Coran et la *Sunna* ⁽²⁾. Dans les faits, les différents courants salafites, ainsi d'ailleurs que les partis islamistes des Frères musulmans, acceptent, par pragmatisme, des accommodements avec leurs discours fondateurs. Mais, une démarcation géopolitique distingue les Frères musulmans égyptiens et En-Nahdha, proches de Qardhaoui, maître à penser du Qatar et les courants salafites, inspirés par le wahhabisme et plus ou moins sous influence, en conséquence, de l'Arabie saoudite.

L'affrontement sur le terrain s'inscrit ainsi dans la concurrence entre les jeux de rôles entre l'Arabie saoudite et le Qatar soucieux de développer leurs influences idéologiques et culturelles au Moyen-Orient et en Afrique du Nord. Ce qui explique l'émergence d'une réaction nationale, dans les pays ciblés, faisant valoir le respect de leurs indépendances. Est-ce à dire que l'Arabie saoudite est « en train de transformer le wahhabisme en une sorte d'église de l'Islam ? » ⁽³⁾. Notons cependant l'existence de nombreux courants salafites : la voie jihadiste, qui préconise la guerre sainte, et le salafisme piétiste, qui privilégie la prédication non violente et des positions intermédiaires, adaptées aux circonstances. Dans ces différents cas, il s'agit de fondamentalistes missionnaires qui usent du *takfir* (accusation de mécréance) et œuvrent pour la réislamisation des populations musulmanes, non acquises à leur lecture littérale.

Fait distinctif, les observateurs associent volontiers aux salafites la défense du port du *nikab* et livrent des batailles contre les institutions qui le contestent, par souci de vérification d'identité, lors des examens, par exemple. En Égypte et en Tunisie, les salafites ont encouragé les manifestations des porteuses de voile : manifestations au Caire et en Alexandrie, en avril 2011 et à Tunis, en décembre 2011.

Les salafites s'émancipent certes des écoles juridiques sunnites. Mais il serait exagéré d'adopter l'affirmation de Bernard Rougier, qui affirme qu'ils « inventent un nouvel islam »⁽⁴⁾. Signalons, dans ce cadre, les relations différentielles des courants salafites dans les pays du Printemps arabe. En dépit de leurs spécificités, les acteurs salafites partagent les vues de la mouvance des Frères musulmans. Ils appartiennent à la même famille politique et définissent, comme ennemis communs, les partisans de l'évolution et du progrès. Mais ils se mobilisent, selon les stratégies et tactiques qu'ils identifient, selon leur appréciation des circonstances, les tempéraments de leurs dirigeants et leur propre éthique de la gouvernance et de l'usage des moyens d'action et des mécanismes de gestion de leurs programmes.

Un front islamiste en Égypte ?

Les salafites faisaient partie des membres de la mouvance islamique pourchassés par le pouvoir. Pis encore, ils étaient volontiers accusés d'être en relation avec le mouvement terroriste *Al-Qaïda*. Plus d'un millier d'entre eux étaient emprisonnés. Leur sortie de prison, après la chute de Moubarak, redynamisait leur mouvement par la reprise en main des anciens dirigeants libérés. Étant donné leurs refus de contester le pouvoir, les courants salafites s'opposaient à la révolution et étaient hostiles aux manifestations de rues. Mais, ils durent réviser leur stratégie depuis la chute du président Moubarak et s'adapter, sous la pression de l'opinion publique, au nouveau contexte. Les salafites participèrent depuis lors aux *sit-ins* de la place Tahrir. Fait plus important, ils acceptèrent de former des partis politiques et de participer aux élections⁽⁵⁾. *Al-Nour Party (Hizb Al-Nour)*, le parti qu'*Ed-Daawa salafia* a pris, après hésitations, l'initiative de fonder, fut reconnu le 12 juin 2011. Refusant d'admettre la révision de leur doctrine, hostile à la démocratie, la citoyenneté et la société civile, ses dirigeants expliquèrent leur nouveau comportement politique par le recours au *fikh al-fourça* (la jurisprudence de la circonstance). Ce subterfuge assurait leur conformité à leur discours fondateur⁽⁶⁾. Néanmoins, les salafites refusèrent toutes alliances avec les partis civils ou de présenter lors des élections des candidats coptes. Mais ils se résignèrent à présenter plus de 60 femmes sur leurs listes, par application de la loi électorale⁽⁶⁾. Groupés désormais en quatre partis : *Al-Nour* (La Lumière), *Al-Assala* (l'authenticité), *Al-Islah* (la réforme) et *Al-Hadhara* (la civilisation), ils se rapprochent en vue de leur unification. Mais l'institutionnalisation ne concerna point la majorité du mouvement⁽⁷⁾.

Les résultats définitifs des élections législatives, proclamées le 21 janvier 2012, ont assuré la réussite du parti salafite, *Al-Nour*, arrivé en deuxième position, avec 96 sièges (environ 20 %), derrière le parti de la Liberté et de la Justice (PLJ) des Frères musulmans qui a obtenu 127 sièges. Les islamistes sont désormais assurés d'accéder au pouvoir. Une alliance entre les deux mouvances, pour former le gouvernement est vraisemblable.

Les variantes du salafisme

En Tunisie, le salafisme s'érigea en acteur important sur la scène politique et organisa de nombreux *sit-ins* et manifestations. Il se présente comme un concurrent du mouvement d'*En-Nahdha*. Mêmes itinéraire des salafistes au Yémen, de l'apolitisme à l'engagement politique. On distingue les courants piétistes (le salafisme quiétiste, le salafisme de mouvement et le salafisme réformiste), qui font allégeance au pouvoir politique (*walî al-amr*) et le salafisme jihadien. Les salafites piétistes ont participé au mouvement contestataire, soutenu le nouveau pouvoir et ont opté pour une participation aux élections, en attendant la formation de leur parti. Leur dirigeant Aquil Maktari a déclaré, dans une interview récente : « Nous reconnaissons les droits politiques de la femme et l'État civil, avec des références musulmanes »⁽⁸⁾.

En Syrie, les salafites participent activement à la lutte contre le régime de Bachar El-Assad. Coopérant avec les dirigeants de la révolution, ils s'adaptent au contexte : ils ont annoncé leur accord, pour l'instauration d'un régime civil, d'un État démocratique pluraliste, d'une égalité entre les citoyens des différentes ethnies ou religions et des exigences de l'État de Droit (déclaration du 26 mars 2012). Mais est-ce qu'il ne s'agirait pas d'une attitude conjoncturelle, d'une concession d'opportunité, susceptible d'être révisée ?

En Palestine, le salafisme jihadien joue son propre jeu. Il participe à la résistance à Gaza. Par contre les salafites des territoires sont d'obédience piétistes. Contenues par le mouvement *Fath*, leurs influences s'exercent essentiellement dans les mosquées⁽⁹⁾.

Au Liban, le mouvement s'est développé depuis le retrait des forces syriennes du pays en 2005. Les salafites sont désormais plus impliqués dans la vie politique où ils s'opposent au mouvement chiïte *Hizb Allah*⁽¹⁰⁾. Saisissant l'occasion de la crise syrienne, les salafites soutiennent les opposants syriens et dénoncent l'attitude du gouvernement qui comprend le *Hezbollah*. Ils appellent aussi les chrétiens à « prendre leur distance » à l'égard de Damas. Mais leur initiative est combattue par *Hizb Allah*, soutien du régime d'El-Assad.

Conclusion

Faut-il s'étonner du triomphe de l'Islam politique, de l'accès au pouvoir des Frères musulmans et de l'émergence du mouvement salafite, dans ses marges, dans une conjoncture de « colère arabe », d'une prise de conscience de la dépendance et de l'islamophobie occidentale ?

À juste titre, Henri Laurens, définit le monde arabe, par « l'émotion et l'appréhension du monde »⁽¹¹⁾. Nous n'excluons pas, dans notre diagnostic, la donne sociale, attestée par le *cursum* des salafites : des marginaux, des déclassés sociaux, qui

appartiennent, le plus souvent, aux populations défavorisées. Le salafisme se développe dans une ère de désespérance sociale et en réaction avec le système dominant. D'une certaine façon, ce comportement politique est une réaction d'indignés.

On assiste désormais à une participation de plus en plus active des salafites à la vie politique. Les ébauches d'institutionnalisation et le passage à l'ère des partis marquent un changement de la donne. Les mouvements salafites réalisent leur conversion progressive, voire leur normalisation. Ils se structurent comme les autres acteurs politiques. Leur victoire, à l'instar des Frères musulmans égyptiens et de l'*En-Nahdha* tunisienne, leur permettra d'accéder à l'*Establishment* et de tirer profit des privilèges de la gouvernance.

Autre scénario possible, celui de la libération des salafites et des Frères musulmans du jeu politique régional, de la concurrence entre l'Arabie et le Qatar. D'autre part, les velléités de prise de pouvoir induit des accommodements significatifs de leurs postulats politiques. Les mutations des salafites d'Égypte, du Yémen et de la Syrie annoncent une remise en cause de la guerre de religion, du rejet de la citoyenneté de la femme et des institutions de la démocratie libérale. Mais des scénarios radicaux et des dérives extrémistes ne peuvent être exclus.

ÉLÉMENTS DE BIBLIOGRAPHIE

- (1) *Ach-Charq al-Awsat*, 18 avril 2011.
- (2) Ridha Belhaj, *Mosaïque FM*, 4 avril 2012.
- (3) Gilles Kepel, *La Presse de Tunisie*, 11 avril 2012.
- (4) Bernard Rougier : *Qu'est-ce que le salafisme ?* ; PUF, Paris, 2008.
- (5) Ali Brahim, *ach-charq, al-awsat*, 6 décembre 2011.
- (6) Hani Nassira, *Al-Hayat*, 30 décembre 2011.
- (7) Mokhtar Chouaïb, *Al-Hayat*, 12 janvier 2012.
- (8) *Charq al-Awsat*, 6, 14 et 19 février 2012.
- (9) *Charq al-Awsat*, 17 avril 2011.
- (10) Omayma Abdel-Latif, Centre Carnegie (<http://carnegieendowment.org>).
- (11) *L'Express*, 21 décembre 2011 - 3 janvier 2012.

À propos d'*Afghanistan*, *guerre lointaine* ?

René Cagnat | Chercheur associé à l'Iris, colonel (er) d'infanterie.

Ce petit livre édité chez L'Harmattan, si discret, si modeste, est important à plus d'un titre. La réflexion qu'il présente à propos de la guerre afghane va très loin. Dans cet ouvrage où cohabitent aisément philosophie, stratégie et théologie, l'auteur, Philippe Conte, s'inspirant notamment du magistère de l'Église catholique, remet en cause non seulement la stratégie américaine et otanienne actuelle mais, au-delà, les errements récents de la civilisation occidentale. « Là-bas (en Afghanistan), l'Occident n'est pas d'abord en butte au terrorisme, il est victime de sa conception erronée de la guerre, de sa conception erronée de la nation, de sa conception erronée du soldat ».

L'auteur commence par s'étonner du fait qu'« après dix années d'intervention des armées les plus modernes et les meilleures du monde, une poignée de "terroristes" continuent leur combat avec l'appui d'une part de plus en plus important de la population ». Réponse : comme au Vietnam, la stratégie des États-Unis imposée à l'Otan est fautive. Traditionnellement le chef militaire américain, sous l'influence de son *lobby* militaro-industriel, privilégie une stratégie des moyens. Face à la violence, il répond par une violence technique encore plus grande : Hiroshima venge Pearl Harbor, l'aviation et ses bombes répliquent aux attentats. On tend ainsi très vite vers une « guerre d'attrition », de destruction aveugle. Le « théorème de Gaza », théorisé par l'armée israélienne dans son combat contre les Palestiniens, en montre toutes les limites : un groupe de 5 activistes est localisé, 2 missiles sont lancés qui tuent 3 militants et en blessent 2 autres ; « combien reste-t-il d'activistes ? Réponse : 10 ! ». En effet, il est prouvé que ce type d'action, loin de l'attrition recherchée, est le meilleur agent recruteur. Pourtant les forces états-uniennes y ont systématiquement recours. Face à une société clanique encore régie par la loi du talion ou la *vendetta*, on ne peut imaginer meilleur facteur d'escalade...

Le commandement américain est pourtant astreint par le « zéro mort » à recourir à l'aviation : 100 morts dans la population importent peu par rapport au décès d'un seul soldat de l'Alliance, qui sera comptabilisé, reproché par une opinion qui comprend mal « que l'on meure pour Karzaï ». Pour éviter les pertes, la troupe ne colle pas à l'adversaire, n'a guère de contact avec la population et sort le moins possible des camps où elle se morfond. Le recours à des mercenaires pour la remplacer n'est qu'un pis-aller tant ces supplétifs sont médiocres. Heureusement, la technologie actuelle ne permet pas encore le recours à des robots mais elle s'y

efforce déjà ! Une question en découle : « Ne sentons-nous pas que nous avons libéré un monstre : une machine de plus en plus autonome, de plus en plus agissante qui écrase l'homme ? ». Le plus clair résultat de cette « dérive technique » est de faire de nos ennemis « l'incarnation de l'homme dressé face à la machine, ce qui relativise la notion de camp du bien » et discrédite l'intervention. L'auteur à ce sujet mentionne une perte du moral qui se traduit chez le combattant et le vétéran par des troubles psychiques, des pulsions suicidaires, etc.

D'où l'injonction de Philippe Conte : « Si notre pays, notre armée, veulent être fidèles à leur vocation, ils doivent permettre à l'Alliance atlantique de réorienter sa stratégie, de découvrir un des enjeux majeurs de la guerre moderne : l'auto-limitation de la puissance de feu ». Il s'agit, face à la violence quelle qu'elle soit, de faire une « réponse en deçà », d'éviter en retour la mort des innocents, de faire la guerre avec mesure, doigté, sinon humanité.

Conte pour cela propose de revenir à la « doctrine chrétienne de la guerre juste » élaborée de Saint Augustin à Saint Thomas d'Aquin, quelque peu oubliée, il est vrai, depuis les années 1940. À son avis, il convient, en dehors de toute volonté de croisade, de mener une guerre imprégnée de respect et de compréhension pour l'ennemi, pour le prisonnier, pour toute victime. En cet adversaire, il faut reconnaître un « ami impitoyable » qui peut nous apprendre beaucoup sur nous-mêmes. À son contact, qu'il faut rechercher, nous devons parler sa langue, nous plier à ses mœurs, si déconcertantes soient-elles. Nous devons gommer de notre comportement tout ce qui peut ressembler à une provocation, percevoir combien ce qui est devenu habituel chez nous est choquant pour l'adversaire : par exemple la présence dans nos rangs de femmes-soldats, si utiles et valeureuses soient-elles. En même temps, nous devons faire preuve de dignité, rester nous-mêmes, montrer à l'adversaire que nous pouvons accepter le combat sur son terrain, être violents comme lui, mais, si possible, en le respectant. Bien entendu l'auteur cite Gallieni, Lyautey et ne manque pas de mentionner que nos coloniaux, même s'ils devaient faire parfois de terribles « exemples », respectaient à peu près les principes ci-dessus. Toute la différence avec les errements actuels réside dans le moral d'acier qui animait leurs corps expéditionnaires et surtout l'autonomie de commandement – pour ne pas dire plus – dont ils bénéficiaient.

« Que sont nos soldats devenus ? ». J'emprunte à Maurice Kopecky ce très beau titre ⁽¹⁾ pour exprimer mon effarement face à l'américanisation et l'asservissement de notre infanterie. Comment reconnaître un chasseur alpin du 27^e BCA dans ce *Rambo* casqué, caparaçonné, surchargé, qui se traîne sur une pente des montagnes de Kapitsa ? C'est le spectre même de la défaite qui menace si nous n'y prenons garde. Comme l'écrivait David Galula, officier français devenu, selon les Américains, « le Clauzewitz de la contre-insurrection » ⁽²⁾, « la guerre révolutionnaire est avant tout une guerre d'infanterie. Paradoxalement, moins les forces loyalistes – anti-insurrectionnelles – sont perfectionnées, meilleures elles sont ».

L'« otanisation », c'est-à-dire, entre autres, la sophistication accélérée de l'armée française lancée fin 2011 en Afghanistan par le programme *Félin* (fantassin à équipements et liaisons intégrées) de numérisation du théâtre d'opérations contredit absolument les exigences de la contre-guérilla. « Chaque combattant est relié en permanence avec sa section. Chacune de ses actions est prise en compte dans un système complètement intégré » ⁽¹⁾. Cela se traduit par un accroissement de la dépendance des compagnies, des sections à la suite de la *Revolution in military affairs* (RMA) qui repose sur une chaîne irréaliste de traitement des données : la haute hiérarchie est noyée sous les informations pendant que les petits échelons voient leurs initiatives bloquées. Est-ce le système de commandement qu'il nous faut sur les théâtres d'opérations qui nous attendent ? Qui plus est, aurons-nous les moyens de financer un tel outil de combat ? S'il faut choisir entre le robot et le soldat, choisissons le soldat fiable, rustique, peu coûteux seul à même de nous défendre corps et âme. Mais en faisant ce choix, rendons-lui la force morale sans laquelle il n'est pas de combattant.

*
**

Au demeurant, en Afghanistan même, l'application des préceptes de la guerre juste et simple prônée par Philippe Conte semble trop tardive pour réussir. Tout cela n'a pas été fait et ne peut plus être fait à temps face à un peuple révolté, définitivement, par l'incompréhension et la brutalité technique manifestées par les États-Uniens. Il faut donc que Français ou Européens (et bien sûr Américains, s'ils se joignent à nous) prennent le large par un repli qui nous rendra liberté de manœuvre et marge d'initiative, ne serait-ce que pour lutter contre le trafic de drogue, notre seul ennemi en Afghanistan. En pays pachtoune, où nous sommes encerclés, ce combat est devenu impossible. En revanche, à partir des marches ouzbèkes et tadjikes de l'Asie centrale, nos Forces spéciales pourront, aux côtés de l'armée russe (qui aura grand besoin d'elles) lutter contre la culture du pavot dans toute la profondeur de l'Afghanistan. Mais il faudra agir avec toute la mesure qu'impose la conduite d'une « guerre juste ». Si nous y parvenons, nos « amis impitoyables » que sont les Afghans nous aurons au moins appris avec quel doigté il faut combattre au XXI^e siècle !

ÉLÉMENTS DE BIBLIOGRAPHIE

(1) Maurice Kopecki : « Que sont nos soldats devenus ? », revue *Espoir* n° 167 de la Fondation de Gaulle, mars 2012 (« Chroniques », p. 78-85).

(2) Titre donné par le général Petraeus, directeur actuel de la CIA, à son introduction à l'ouvrage majeur de Gallula : *Contre-insurrection, théorie et pratique* ; Éditions Économica, 2008.

Stratégie maritime intégrale : une approche conceptuelle

Lars Wedin | Capitaine de vaisseau ® de la Marine royale suédoise. Membre de l'Académie royale suédoise des sciences de la guerre. Chercheur à l'Institut français d'analyse stratégique (Ifas) et chercheur associé au Collège de défense suédois.

La mer est vitale pour l'humanité : 70 % de la population mondiale vit près de la mer et 2 milliards de personnes sont directement dépendantes de la mer qui leur fournit leur alimentation. Dans le monde d'aujourd'hui, connecté et mondialisé, l'économie est dépendante de communications maritimes sûres et sécurisées. C'est à n'en pas douter le cas de l'Union européenne : 90 % de son commerce extérieur et 40 % de ses échanges commerciaux intérieurs sont transportés par voie maritime. Ce sont des chiffres qui vont en outre augmenter avec le projet des autoroutes de la mer. L'UE est aussi de plus en plus dépendante du gaz naturel provenant des gazoducs sous-marins, comme le *Nord Stream* en mer Baltique. L'opération de l'Otan en Lybie, baptisée *Unified Protector*, dépendait largement de la mer : porte-avions, bombardement des côtes, déminage et blocus.

Malheureusement, la mer est également le lieu de nombreuses activités illégales : traite d'êtres humains, piraterie, pêche illégale, etc. Enfin, les problématiques environnementales prennent de plus en plus d'importance et affectent non seulement le transport maritime et la pêche mais également les activités navales. Ces dernières nécessitent une certaine régulation pour que la mer puisse continuer à être utilisée en tant que ressource mondiale dont tout le monde doit pouvoir bénéficier.

Dans ce contexte, il est important de définir des objectifs politiques cohérents et des stratégies permettant de les atteindre. Ces stratégies devront tenir compte à la fois des aspects civils et militaires, y compris navals. Nous avons besoin d'une approche globale de la stratégie maritime. Nous prendrons ici l'UE en guise d'exemple mais les propos pourront facilement être transposés à n'importe quel pays maritime.

Corbett ne suffit pas

On doit la définition classique de la stratégie maritime à Corbett : « Par stratégie maritime nous entendons les principes qui gouvernent une guerre où la mer reste un facteur d'importance ». Cette définition n'est pas très utile dans le monde d'aujourd'hui, dans la mesure où il s'agit d'une stratégie de guerre, c'est-à-dire une situation fort improbable, même si ce n'est pas une situation impossible.

Sa définition de la maîtrise de la mer (on parle aujourd'hui de contrôle de la mer) n'est pas non plus tout à fait adaptée : « La maîtrise de la mer ne signifie rien d'autre que le contrôle des communications maritimes... ». Castex donne, lui aussi, la priorité aux communications : « La maîtrise de la mer signifie le contrôle des communications essentielles de surface ».

Aujourd'hui cependant la mer, fonds marins compris, est devenue de plus en plus importante. Le pétrole, le gaz, les gazoducs, les élevages piscicoles et autres ressources, ainsi que les éoliennes, les installations d'énergie marémotrice ou hou-lomotrice constituent des actifs qui requièrent sûreté et sécurité. On pourrait avancer que cela conduit à une territorialisation – ou mieux une infrastructurisation – de la mer. Il ne suffit plus à défendre les communications ; la mer elle-même a besoin d'être défendue.

Par conséquent, il nous faut une nouvelle définition de la stratégie maritime. Sur la base des théories du général Lucien Poirier, on peut définir la stratégie maritime comme « la science et l'art de manœuvrer des forces maritimes afin d'atteindre les objectifs politique dans le domaine maritime ». Ici « forces » signifient tous les moyens – civils et militaires – existants et potentiels. Le terme « manœuvrer » implique utiliser ou employer des « forces » dans un sens très large.

Objectifs politiques et projets

Les forces navales ont un rôle dual unique. Elles font partie des moyens interarmées mais appartiennent aussi au monde maritime. L'officier de Marine doit avoir un comportement professionnel à la fois dans les milieux militaires et des milieux maritimes. Ainsi, on peut distinguer deux grandes catégories d'objectifs politiques dans le contexte maritime. La première concerne le domaine maritime lui-même, le second ne le concerne pas. L'opération *Atalanta* par exemple appartient à la première catégorie : elle est mue par des demandes du secteur maritime. En revanche, l'opération *Unified Protector* ne l'était pas, même si elle était largement dépendante de la mer. Il y a sans aucun doute un lien entre les deux, puisque toutes deux nécessitent la même chose, à savoir des forces navales modernes et polyvalentes. Nous discuterons ici de la première catégorie, puisqu'elle pose des problèmes complexes d'un point de vue conceptuel.

« La politique maritime intégrée pour l'Union européenne » constitue un projet politique pratique pour la première catégorie. Dans le préambule, il est stipulé que « toutes les questions relatives aux océans et aux mers d'Europe sont liées entre elles et que les politiques maritimes doivent être élaborées conjointement si nous voulons obtenir les résultats escomptés ». En outre, la politique « renforcera la capacité de l'Europe à faire face à la mondialisation et la compétitivité, au changement climatique, à la détérioration du milieu marin, à la sécurité et à la sûreté maritime, ainsi qu'à la sécurité énergétique et à l'utilisation durable de l'énergie » (Com 2007, 574 final). Cela se traduit par toute une série de projets, comme un

espace maritime européen sans barrières et une stratégie européenne pour la recherche marine. Cependant, il ne s'agit pas d'une véritable politique intégrée parce qu'elle englobe seulement des actions du premier pilier. Elle ne comprend pas les actions des marines de guerre et des garde-côtes.

Est-il possible de les intégrer dans une stratégie ? La plus grande partie de ces politiques, projets et stratégies ne sont pas vraiment des stratégies au sens que Beaufre leur assigne : « La stratégie est donc l'art dialectique des forces ou encore plus exactement l'art de la dialectique des volontés employant la force pour résoudre leur conflit ». Cependant, ces stratégies forment le volet demande de l'équation stratégique de l'UE ; elles posent les exigences de la manœuvre stratégique dans le domaine de la sécurité. De fait, une telle stratégie, comprenant un recours éventuel à la force armée, constitue le chaînon manquant de cette politique, malgré l'utilisation du mot « sécurité » dans le préambule de la politique maritime intégrée.

Une stratégie maritime générale

Le véritable défi, en particulier dans le contexte de l'UE, consiste à créer une stratégie globale qui tiendrait compte de tous ces aspects. C'est ce que nous appelons une stratégie maritime intégrale : la stratégie maritime intégrale (de l'UE) a pour vocation de développer, encourager et défendre nos intérêts à la mer. Elle coordonne toutes les activités et toutes les forces dans le domaine maritime afin de mettre en œuvre la Politique maritime intégrée.

Cette stratégie est soutenue par, et requiert des résultats des stratégies et projets économiques, environnementaux, etc. ; mentionnés ci-dessus d'une part, et d'autre part, une stratégie d'action, qui est « une véritable stratégie » au sens de Beaufre. Nous pourrions l'appeler stratégie d'action maritime : « La stratégie d'action maritime soutient, sous toutes les conditions, la stratégie maritime intégrale en contribuant à la sûreté, la sécurité et l'utilisation légale de nos communications maritimes ainsi que toutes nos autres installations en mer et dans les fonds marins. En cas de crise et de conflit, elle va aussi interdire l'utilisation de la mer à notre adversaire et influencer ses actions sur terre. La stratégie utilise et coordonne toutes les forces maritimes – civiles et militaires, existantes comme potentielles ».

La stratégie d'action maritime peut être divisée en stratégies opérationnelles ou en missions stratégiques, d'une part et en stratégie de ressources, d'autre part. La mission de cette dernière est de développer, d'acquérir et d'entraîner les forces maritimes nécessaires à la mise en œuvre des missions stratégiques. Concernant les stratégies opérationnelles, les cinq missions stratégiques déclarées dans le *Livre blanc* de 2008 pourraient être un point de départ utile : connaissance et anticipation, dissuasion, prévention, protection et intervention.

La surveillance maritime est un sujet clé dans le cadre de la première mission. Elle devrait conduire à la *Maritime Domain Awareness (MDA)*, définie comme la compréhension effective de toute chose associée au domaine maritime et susceptible d'avoir un impact sur la sécurité, la sûreté, l'économie ou l'environnement. La *MDA* requiert la fusion du renseignement et des données civils et militaires, dans le respect de la confidentialité, par exemple concernant la localisation des sous-marins ou l'intégrité de la personne.

Ci-dessous, quelques exemples sur la manière dont ces missions stratégiques peuvent être liées à des missions et des tâches opérationnelles et tactiques.

Mission	Marine	Garde-côtes
Connaissance et anticipation	Surveillance, renseignement, études et analyses stratégiques et océanographiques	
Dissuasion	Présence, exercices, démonstrations de puissance	
Prévention	Déploiement, exercices internationaux, présence	Patrouilles, inspections de sécurité
Protection	Maîtrise de la mer, convois	Activités selon la <i>CSI (Container Security Initiative)</i> , recherche et sauvetage
Intervention	Projection de puissance, acquisition de la maîtrise de mer, interdiction.	Actions de police, interdiction

La présence vigilante est une mission fondamentale, qui se trouve à la base de toutes les missions. Les forces navales modernes ont une portée colossale, en mer et sur terre, grâce à leurs systèmes de communication, de surveillance et d'armes. Cependant, bon nombre de missions requièrent une présence physique à un endroit donné, par exemple dans le cadre d'un blocus.

Une stratégie d'influence

Pour garantir la nécessaire réglementation de l'utilisation de la mer et sa préservation en tant que ressource mondiale, il faut plus qu'une stratégie d'action. Il faut également une stratégie d'influence. Aujourd'hui, la puissance est de moins en moins militaire, elle repose de plus en plus sur la capacité à rassembler des soutiens par des réseaux et des acteurs non étatiques, entre autres.

Une flotte marchande moderne, bien entretenue et respectueuse de l'environnement constitue indéniablement un élément important d'autorité stratégique. La recherche maritime de haut niveau constitue l'un des fondements indispensables à l'action politique.

Les marines et les garde-côtes peuvent sans aucun doute contribuer à une telle stratégie grâce à la diplomatie navale : la présence, les visites de ports, les exercices internationaux sont des activités importantes susceptibles de soutenir une stratégie politique d'influence.

La puissance d'influence requiert crédibilité et légitimité. Ce qui, à son tour, requiert des actions concertées dans les domaines politiques, diplomatiques et maritimes, y compris dans le domaine naval, mais aussi dans les domaines économique et environnemental. Ceci appelle enfin une stratégie politique au plus haut niveau, une stratégie maritime générale. S'il est difficile d'élaborer ce type de stratégie au niveau national, ça l'est d'autant plus au niveau européen. Mais il faut essayer.

Rassembler tous les éléments

Pour réaliser la politique maritime intégrée de l'Union, l'industrie maritime européenne doit être compétitive, tout en respectant les nécessités environnementales. La mise en œuvre du projet des autoroutes de la mer, parallèlement à la création d'un espace maritime sans barrières, constituerait un pas important dans la bonne direction. En outre, il faut communiquer l'importance de la mer au grand public, afin de guérir les populations de cette maladie trop répandue qu'est « l'aveuglement de la mer ».

Parallèlement à cette politique, il faut une stratégie maritime d'action. Il faut créer une surveillance, une *Maritime Domain Awareness (MDA)* dans les mers voisines de l'Europe. Dans ces eaux, l'Europe doit disposer des moyens de protéger le commerce et ses autres actifs, en termes de sécurité et de sûreté. L'Europe doit également être capable de prévenir les activités illégales, en particulier la traite des êtres humains, grâce à une véritable capacité d'intervention.

Les intérêts maritimes de l'Europe ne s'arrêtent pas aux mers voisines. Pour y pourvoir, il faut faire preuve de réactivité, c'est-à-dire être prêt à protéger et à intervenir, ce qui requiert à son tour au moins une certaine présence, avec des forces maritimes modernes et bien formées. Dans la mesure où les ressources de l'Europe sont maigres, la prévention sous forme de coopération et de diplomatie navale est de première importance.

Plus généralement, l'Europe doit influencer le développement naval afin de garantir la protection des grandes ressources mondiales pour l'avenir de l'humanité.

Là aussi, cela requiert de la diplomatie navale mais surtout une action politique et diplomatique concertée.

Pour atteindre ces objectifs, les questions maritimes doivent faire partie des priorités politiques. Il faut penser en termes globaux, sans créer de barrières artificielles entre les différents types de forces maritimes.

*

**

L'approche structurée proposée ici permettrait d'analyser, de comparer et de discuter des stratégies et des objectifs afin de déterminer où se trouvent les contradictions et les conflits pour évaluer leur efficacité générale. Les résultats permettraient notamment de mettre en lumière le manque de ressources. C'est un problème récurrent qui sera aggravé par la réduction des budgets du fait de la crise économique.

Le fossé qui existe entre les activités civiles et militaires constitue un problème fondamental dans le domaine maritime. De nombreux pays et organisations distinguent de manière stricte ce qui relève du militaire et ce qui relève du civil, sans comprendre que le « maritime » s'étend, de part et d'autre, de cette séparation. L'Otan par exemple n'a pas vraiment de lien direct avec le monde maritime civil. L'UE quant à elle, est toujours, malgré le Traité de Lisbonne, divisée en trois piliers traditionnels. C'est la Commission européenne qui a élaboré le projet de politique maritime intégrée et elle n'a pas son mot à dire sur les affaires militaires ou navales. Cela dit, la mer est d'abord un tout. En conséquence, une stratégie maritime générale doit être abordée au plus haut niveau politique et elle doit être absolument complète. Cela nécessite une prise de conscience de l'importance vitale de la mer, non seulement pour l'Europe mais pour l'humanité tout entière.

Le *New START Treaty* : un traité nécessaire ou dépassé ?

Steven Ekovich | Professeur à l'AUP, *The American University of Paris*.

Lors du Sommet sur la sécurité à Séoul le 26 mars 2012, le président Obama a précisé à voix basse et confidentielle au président russe Dmitri Medvedev qu'il aurait « plus de flexibilité » pour traiter des questions controversées telles que la défense antimissile après l'élection présidentielle de 2012, et que le futur président russe Vladimir Poutine devait lui donner du champ (de la « marge de manœuvre »). Medvedev a répondu qu'il comprenait (« je suis avec vous ») et qu'il allait transmettre les remarques à « Vladimir ». L'échange chuchoté a été néanmoins repris par les micros des journalistes qui entraient dans la salle. Dans une atmosphère surchauffée de campagne présidentielle, les propos *sotto voce* captés par les micros ont suscité une vive polémique aux États-Unis.

Controverses sur la défense antimissile

L'opposition républicaine s'est empressée d'accuser le Président de s'approprier à trahir la sécurité nationale américaine dès que l'occupant de la Maison-Blanche serait libéré de la pression électorale. Cette critique est bien résumée par le président de la Chambre de Représentants, John Boehner, qui a néanmoins attendu le retour du Président avant de lui envoyer une lettre vive quelques jours plus tard. Le chef de file du Parti républicain à la chambre basse clame son indignation.

« Le programme de défense antimissile des États-Unis est essentiel à notre sécurité intérieure et à la sécurité collective de nos partenaires de l'Otan, et elle a des implications claires pour la sécurité de nos alliés au Moyen-Orient. Moi-même et d'autres membres de la Chambre de Représentants avons déjà exprimé notre préoccupation quant à la volonté apparente de votre administration à faire des concessions unilatérales à la Russie qui minent nos capacités de défense antimissile. Vos commentaires renforcent ces inquiétudes. Le gouvernement russe n'a pas respecté ses obligations de se rallier à la communauté internationale dans son opposition aux États voyous d'Iran, de Syrie et de Corée du Nord. Au contraire, Moscou a parfois offert son soutien à ces régimes dangereux. Et il est de plus en plus évident que la Russie a l'intention d'étendre ses frontières et son pouvoir par des actes hostiles, y compris l'invasion d'un pays voisin allié des Américains [lire ici la Géorgie]. Il est troublant de constater que vous suggérez aux dirigeants russes que

leur ambition imprudente serait récompensée par la « flexibilité » sur notre programme de défense antimissile après la prochaine élection. Cela a des implications importantes pour la sécurité de notre patrie, envoie un signal terrible à nos alliés partout dans le monde et remet en question l'efficacité de votre politique de « *Reset* » avec le gouvernement russe ».

Le très probable candidat à l'investiture du parti Républicain, Mitt Romney, lui a emboîté le pas et lourdement, en déclarant que la Russie reste l'adversaire numéro « un » des États-Unis. Sa déclaration a tout de suite été tournée en ridicule par l'équipe de sécurité nationale de la Maison-Blanche ainsi que par les géostratèges chevronnés du Parti démocrate.

Les défenseurs du président Obama ont riposté en affirmant que le sens de ses propos chuchotés relevait tout simplement de l'évidence : la complexité du dossier exige un laps de temps assez large et, par conséquent, une sérénité diplomatique ; de telles questions ne pourraient pas être traitées dans l'atmosphère hyperpartisane d'une campagne présidentielle. En outre, ajoutent-ils, le budget militaire que la Maison-Blanche a soumis au Congrès en février dernier réduit bon nombre de projets de grande envergure mais il maintient les 9,7 milliards de dollars consacrés à la défense antimissile (avec des provisions s'élevant à 47,4 milliards au cours des cinq prochaines années). En d'autres termes, une telle enveloppe budgétaire signifie que le Président n'est pas disposé à céder aux Russes sur le bouclier antimissile. En plus, lors du Sommet de l'Otan à Chicago fin mai 2012, un point de l'ordre du jour est consacré à l'annonce que le système de défense antimissile aura atteint « une capacité opérationnelle provisoire » ; c'est-à-dire que le programme est déjà bien lancé. L'*USS Monterey*, un croiseur conçu pour offrir un système de défense contre les missiles balistiques, sera opérationnel dans le bassin méditerranéen. L'Espagne accepte de servir de port d'attache pour quatre autres bâtiments de ce type. Dans le même temps, un système d'alerte radar sera mis en opération à la base de Kurecik en Turquie. Des accords ont également été signés avec la Roumanie et la Pologne pour servir de sites pour des missiles intercepteurs respectivement dès 2015 et 2018. Alors, répondent ceux qui relativisent les propos d'Obama face à Medvedev, pourquoi le Président aurait-il pris la peine de dépenser tout cet argent, de procéder à la refonte de tous ces navires et d'organiser tous ces accords de l'Otan, s'il avait l'intention de jeter par-dessus bord le bouclier antimissile ?

Le contexte géopolitique et historique qui a préparé le terrain à une telle polémique nous renseigne sur la culture stratégique des États-Unis et les inflexions que Barack Obama essaie d'y apporter. L'arrivée de Barack Obama à la Maison-Blanche a suscité de grandes attentes. Après tout, le slogan « *Change we can believe in* » était au cœur de sa campagne présidentielle. Au nombre des changements de cap attendus figuraient de nouvelles orientations en matière de politique étrangère. Toutefois, on constate beaucoup plus de continuité dans les relations des États-Unis avec le reste du monde que de véritables transformations profondes. Il est indiscutable que l'élection d'un Président dont le père était africain a redonné

de l'éclat à l'image des États-Unis. Certes une image positive constitue un atout diplomatique. Il n'est pas mauvais de redorer le blason d'un pays mais chaque État possède ses intérêts propres, défendus et mis en avant par une panoplie d'institutions et de processus qui ne changent pas d'un jour à l'autre. De plus, les forces en place dans le monde ne sont pas si facilement malléables même par une grande puissance. Les entraves de la politique intérieure et extérieure ont réduit la vraie marge de manœuvre du Président américain. Même les secousses d'origine extérieure, comme les soulèvements arabes, ne parviennent pas à ébranler les vecteurs fondamentaux de la politique étrangère des États-Unis. Toutefois, s'il est un dossier où apparaît une tentative de vrai changement, et sur lequel Obama s'est efforcé d'apporter un infléchissement, c'est celui concernant la Russie. C'est la signature par les deux anciens rivaux, d'un traité prévoyant une réduction réciproque des armes nucléaires, qui constitue l'effort le plus substantiel de cette nouvelle démarche.

Le traité en question, le *New START Treaty*, se trouve au cœur des efforts de la Maison-Blanche pour relancer les relations russo-américaines vers une entente plus posée.

Un nouveau traité russo-américain de réduction des armes stratégiques

Le traité qu'il faut considérer ici alors est un accord entre les États-Unis et la Fédération de Russie, dont la rédaction a commencé en avril 2009 après la rencontre des présidents Barack Obama et Dimitri Medvedev à Londres. Il fut ensuite signé le 8 avril 2010 à Prague et, conformément à la Constitution américaine, ratifié par le Sénat le 22 décembre de la même année. Il est entré en vigueur le 5 février 2011 et encadrera la réduction d'armes nucléaires au moins jusqu'en 2021. Le *New START* constitue la suite des traités *START I* et *START II*. *START* est l'acronyme de l'anglais *Strategic Arms Reduction Treaty* (Traité de réduction des armes stratégiques). Tous les traités *START* visent à réduire substantiellement les arsenaux nucléaires américain, soviétique puis russe (aussi bien les ogives portées par les missiles terrestres que sous-marins et aériens). *START I*, lancé par le président Ronald Reagan, fut signé en juillet 1991 et entra en vigueur en décembre 1994. Il a expiré le 5 décembre 2009 mais a été reconduit temporairement. *START I* est devenu un des traités de contrôle d'armements le plus complexe de l'histoire. Sa mise en œuvre a encadré le retrait d'environ 80 % de toutes les armes nucléaires stratégiques de l'époque.

Après la signature de *START I* en 1991, les États-Unis et la Russie ont entamé les négociations qui ont amené les deux parties à signer *START II* en 1993, ratifié par les États-Unis en 1996 et par la Russie en 2000. Le parlement russe a temporisé et retardé la signature en signe de protestation contre les bombardements de l'Otan en ex-Yougoslavie, la guerre en Irak et l'élargissement de l'Otan. *START II* prévoit la poursuite de la réduction des arsenaux stratégiques dans des

proportions importantes – jusqu’aux deux tiers. Un élément central concerne l’abandon de missiles à têtes multiples, les *MIRV* (*Multiple Independently Targetable Reentry Vehicle* – le « mirvage » – un missile à plusieurs têtes nucléaires qui suivent chacune leur trajectoire lors de leur entrée dans l’atmosphère). Mais *START II*, bien que ratifié, n’a jamais été appliqué car la Russie veillait à ce que les Américains maintiennent en vigueur le Traité *ABM* de 1972 sur la limitation des missiles anti-missiles balistiques, une condition russe impérative de sa ratification. La Maison-Blanche de George W. Bush s’étant retirée du Traité *ABM*, a rendu *START II* lettre morte.

Toutefois, *START II* était déjà *de facto* dépassé en raison des mesures de réduction unilatérale des arsenaux annoncées en novembre 2001 par les présidents russe et américain. Malgré le nouvel état de fait, un autre traité, Le *Strategic Offensive Reductions Treaty* (*SORT* – Traité de réduction des arsenaux nucléaires stratégiques offensifs) a abaissé davantage les plafonds fixés par *START II* mais a été de toute façon dépassé par les événements. Donc *SORT* constitue une évolution de *START II*, destinée à céder place éventuellement à un traité *START III*. *SORT* est entré en vigueur en juin 2003 et aurait expiré le 31 décembre 2012, s’il n’avait pas été remplacé par le *New START* qui est essentiellement une variante d’un hypothétique *START III* issu de *SORT*.

Mais au lieu de porter le nom *START III*, ou même celui provisoire mais encombrant de *Measures for the Further Reduction and Limitation of Strategic Offensive Arms*, cette nouvelle version de la série des traités de réductions des armes stratégiques est rebaptisée « *New* » *START* par la Maison-Blanche. Cette nouvelle appellation a certainement été adoptée dans un but de relations publiques ou en guise de geste symbolique diplomatique, afin d’appuyer la nouvelle démarche de Barack Obama auprès de la Russie. L’adjectif « *New* » rime bien avec la stratégie, déjà mise en place, de « *Reset* » des relations entre les anciennes puissances rivales ; le terme « *Reset* » étant un emprunt au langage informatique qui signifie « relancer, redémarrer ». Il s’agit ici d’oublier tous les contentieux et faire table rase du passé pour ouvrir une nouvelle ère diplomatique entre les États-Unis et la Russie.

Que faut-il penser de ce traité ? Cosmétique ou décisif ?

Les critiques, qui n’ont pas tardé à fuser, accusaient de nouveau Barack Obama de cantonner sa politique étrangère au strict maniement des symboles aux dépens d’intérêts concrets des États-Unis. La question est donc de savoir si ce traité est réellement nécessaire (ou n’est-il qu’un vestige de la guerre froide), autrement dit, s’il est en vérité dépassé, voire même ringard. Pour certains opposants, ce nouveau traité n’est pas seulement suranné mais il s’aligne dangereusement sur les intérêts et visées russes, procurant peu d’avantages du côté américain. En outre, il semble que ce traité soit pour Obama un pas vers sa vision à long terme d’éradication totale des armes nucléaires, même si dans l’immédiat il constitue bien une étape

de la relance des relations entre les deux pays. Ce volet-là de la mise en avant du *New START* est largement vu comme angélique et naïf ou tout au moins utopique.

Afin de bien démêler les arguments pour ou contre le traité, il convient de faire un bref rappel des négociations stratégiques entre Washington et Moscou. En pleine guerre froide, les négociations ont d'abord porté sur la limitation du nombre de missiles nucléaires avec les deux traités *SALT* (*Strategic Arms Limitation Treaty*), pour ensuite passer à une réduction significative de ces armes. Les traités *SALT* avaient pour objectif de contrôler l'escalade du nombre d'armes en établissant les plafonds au-delà desquels les deux puissances n'avaient plus le droit d'augmenter leurs arsenaux nucléaires. Mais même le simple plafonnement des armements nucléaires nécessitait la poursuite d'une politique de détente entre Washington et Moscou. C'est seulement avec la fin de la guerre froide qu'il est devenu envisageable de passer de la simple limitation des armes nucléaires à leur réduction. C'est ainsi qu'aux traités *SALT* ont succédé les traités *START*, lesquels ont vraiment contribué à une nette diminution des missiles et des têtes nucléaires des deux parties. Il faut cependant souligner que les traités n'ont fait que contribuer à la réduction des armes nucléaires. Aux yeux de certains, c'était tout simplement la fin de la compétition entre protagonistes nucléaires qui rendait superflue la détention d'une telle quantité d'armes. Leur relatif abandon était donc la conséquence naturelle de l'atténuation de l'affrontement. En d'autres termes, certains disent que les traités *START* n'auraient fait qu'entériner le nouvel ordre des choses.

Le débat autour du traité a fait ressortir diverses critiques ainsi que des arguments à l'appui. Pour bien situer le débat, il ne faut pas perdre de vue les enjeux de politique intérieure et électorale, qui influent toujours sur la politique extérieure. En ce qui concerne le « *Reset* » entre la Russie et les États-Unis, on peut dire qu'en faisant des concessions, la Maison-Blanche a voulu signifier aux Russes que ceux-ci étaient encore une puissance nucléaire qui comptait et que, s'il restait un domaine où ils pouvaient prétendre détenir le statut d'une grande puissance crédible, de ne pas être relégués au second rôle, c'était bien celui du nucléaire. À ce titre, ils pouvaient continuer de jouer un rôle principal dans les affaires diplomatiques et stratégiques de la vie internationale. En bref, il s'agissait pour rassurer les Russes de les inviter à venir jouer un rôle de premier ordre sur la scène des grandes puissances. Autrement dit, la possession d'un arsenal d'armes nucléaires confère à la Russie le droit de « voyager en première classe » dans les sphères diplomatiques, de ne pas être déclassée vers la « classe affaires » occupée par les puissances pétrolières, et surtout pas dans la « classe économique » ce qui refléterait cruellement sa situation financière actuelle, pour le moins délicate. Alors évidemment, pour la Maison-Blanche, ce traité n'est non seulement pas ringard mais bien nécessaire au redémarrage des relations entre Washington et Moscou. Sur un certain plan, quelques éléments de critique de l'aile gauche du Parti démocrate rejoignent la critique de l'aile droite du parti Républicain. Les deux extrêmes de l'éventail idéologique sont au moins d'accord pour considérer que le traité *New START* est

dépassé car il est, dans ses termes mêmes, un vestige de la guerre froide. Pour la gauche le traité ne va pas assez loin dans la finalité souhaitée d'éliminer les armes nucléaires. Mais le flanc gauche d'Obama estime que, malgré ses insuffisances liées à son caractère suranné, le traité est nécessaire dans la mesure où il fait partie d'un tissu d'accords très complexes, consacré aux armements nucléaires et à leur non prolifération. En revanche, l'aile droite du Parti républicain considère que ce traité est tout à la fois ringard, inutile et même dangereux car il ne fait que fragiliser la position stratégique des États-Unis. La droite reste interloquée de la posture paranoïaque des Russes qui ont, manifestement, besoin d'être rassurés sur de supposées intentions américaines à leur encontre. Pour la droite américaine, le traité *New START* n'a plus de justification puisque les problèmes de la guerre froide n'existent plus. Il conviendrait plutôt d'adopter une posture défensive, stratégique et nucléaire en mesure de dissuader d'éventuelles menaces venants du terrorisme nucléaire, de l'Iran, de la Chine et de la Corée du Nord, et cesser d'entretenir des négociations diplomatico-thérapeutiques avec les Russes – d'autant plus que les accords de ce traité ne concernent pas les armes tactiques nucléaires des Russes (majoritaires en nombre) – ni la sécurité de celles qui existent encore, ni même l'éventualité qu'un groupe non étatique puisse s'emparer d'une tête nucléaire avec intention de menacer directement le territoire américain.

Ambiguïtés, compensations, arrière-pensées

Une des concessions qui a conduit au traité et qui inquiète la droite républicaine concerne le bouclier antimissile envisagé en République Tchèque et en Pologne et que Barack Obama a provisoirement ajourné, se ralliant ainsi à la position russe. Pour la Maison-Blanche, cet abandon fait partie d'une politique de petits pas pour restaurer une certaine confiance entre les États-Unis, l'Otan et la Russie en vue néanmoins d'un éventuel système antimissile intégré moins proche de la frontière russe. Qu'attendaient les Américains en retour ? En échange de leur concession sur le bouclier antimissile, Washington souhaitait une coopération accrue des Russes dans la lutte contre le terrorisme ainsi que la continuation de l'utilisation du couloir aérien russe pour acheminer toutes la logistique otanienne vers l'Afghanistan. Les critiques rétorquent que, de toute façon, la coopération russo-américaine dans la lutte contre le terrorisme est déjà très solide étant donné que les deux pays partagent le même intérêt vital en la matière. De plus, en relevant que les Russes ne souhaitent pas réellement voir la défaite de l'Otan en Afghanistan, ils n'ont pas intérêt à faire obstacle à l'approvisionnement des forces déployées. Cela n'empêche pas que le Kremlin voudrait voir traîner le conflit en Afghanistan afin d'affaiblir l'Otan.

Les adversaires du traité se demandent si les États-Unis ont recueilli les fruits escomptés d'un tel accord. Au moins, ont-ils l'espoir de voir certains dirigeants russes modérer leurs propos à leur égard. Espoir perdu en vue de la forte dose d'anti-américanisme que comportait la campagne électorale récente de

Vladimir Poutine. Une certaine déception s'est donc fait jour puisque la réponse symétrique attendue n'est pas venue et on soupçonne fortement que le « *Reset* » se révèle plus favorable à la Russie qu'aux États-Unis. Néanmoins, il serait bon de rappeler que, par le passé, des accords fructueux ont été signés sans pour autant bénéficier d'une atmosphère harmonieuse de respect mutuel. Le traité *START II* a été ratifié entre les États-Unis et la Russie dans des contextes de discussions peu favorables, qu'il s'agisse des bombardements en Yougoslavie, de la guerre d'Irak ou de l'expansion de l'Otan. Il faut aussi rappeler que le traité *START II* n'a jamais été appliqué car la condition *sine qua non* posée par les Russes à sa mise en œuvre était que les Américains préservent le traité de missiles antibalistiques (*ABM*), ce que Washington n'a pas honoré. Ce contentieux a resurgi dans les interprétations du *New START*, notamment en ce qui concerne le lien entre missiles offensifs et missiles défensifs. Dans la mesure où un nombre réduit de missiles offensifs pouvait être plus facilement neutralisé par un solide système antimissile, il s'agit d'une cause de profonde inquiétude. Par conséquent, les Russes ont apposé leur interprétation de ce volet du traité — qui est insérée d'une façon plutôt ambiguë dans le préambule — et qui ne rejoint pas du tout le sens donné par les Américains. Il y a clairement ici une mésentente. Ce traité stipule aussi que les Américains gardent le droit de stocker des têtes nucléaires non déployées en cas de besoin, ceci dans une logique de dissuasion nucléaire. *New START* intègre donc cet élément de *SORT* : le droit de stocker des ogives retirées au lieu de les détruire. Une telle disposition avait déjà profondément contrarié Moscou par le passé.

Pour les adversaires de ce traité, le contentieux russo-américain sur le lien entre armes offensives nucléaires et bouclier antimissiles persiste et des clarifications s'imposent. Les opposants s'insurgent contre tout affaiblissement de défense antimissile face aux armes nucléaires offensives. Le Sénat, qui est constitutionnellement chargé de « donner son avis et son consentement » à tout traité, a accepté de ratifier *New START* en attachant à son vote une déclaration interprétative séparant clairement tout lien entre défense antimissile et réduction de missiles offensifs. Cette déclaration a permis de rallier un nombre suffisant de sénateurs républicains hésitants afin d'obtenir les deux tiers des votes nécessaires (le vote final était 71-26) pour faire gagner la Maison-Blanche. Outre ces clarifications et interprétations lors des débats, l'appui des militaires américains en faveur de la ratification fut déterminant dans la décision des sénateurs. Le Pentagone a trouvé son compte dans le traité, surtout parce qu'il permet la réouverture des installations russes à la vérification ; ce qui n'était plus le cas après l'expiration du précédent traité. En politique intérieure, il est clair aussi que les Républicains ne voulaient pas laisser l'occasion d'une victoire à Barack Obama. Même ceux qui se sont finalement rangés du côté d'une ratification ont protesté, prétendant ne pas avoir été consultés ni informés pendant les négociations et la rédaction du traité, comme le veut la tradition sénatoriale. Les sénateurs réfractaires qui ont voté pour le traité peuvent se vanter d'avoir donné à leur pays l'assurance que les Américains garderaient toute liberté de construire leur propre système de défense antimissile.

Une autre contrepartie arrachée par les sénateurs hésitants a été l'augmentation du budget de la défense dans ce secteur pour renouveler et moderniser l'arsenal nucléaire existant. De même, ce traité n'exclut pas la possibilité pour les Américains, à l'avenir, de recourir à d'autres systèmes stratégiques non nucléaires. Rien ne dit, cependant, que les Russes comprendront le traité dans ce sens, ce qui risque de perturber les relations futures. Dans une déclaration unilatérale sur le nouveau traité *START*, Moscou a déclaré qu'il existe bien une relation entre les armes offensives et défensives et qu'il se réserverait le droit de se retirer du traité si les États-Unis construisaient leurs défenses au point de devenir une menace pour le potentiel de frappe nucléaire russe. Certains Républicains ont affirmé à grands cris que les Russes avaient l'intention de miner le programme de défense antimissile. En réaction, l'Administration Obama a énoncé sa propre déclaration unilatérale, en prenant note de l'inquiétude russe mais en ajoutant que les défenses antimissile américaines « ne sont pas destinées à influencer sur l'équilibre stratégique avec la Russie » mais plutôt destinées à se défendre contre une frappe limitée à partir des « menaces régionales », et que, à cette fin, les États-Unis allaient « continuer à améliorer et déployer de tels systèmes ». Bien entendu, il a été aussi clairement noté par tous les parties que les déclarations unilatérales à propos d'un traité n'ont aucun effet juridiquement contraignant.

Perceptions et cultures stratégiques

Alors, il est évident qu'il s'avère difficile de convaincre les Russes que l'approche de Washington est vraiment en rupture avec la stratégie d'endiguement, stratégie bien antérieure au commencement de la guerre froide, et qu'on peut trouver déjà dans les écrits du géopoliticien américain Nicholas J. Spykman, disciple critique de son prédécesseur et compatriote Alfred Mahan, et continuateur de l'approche géostratégique du Britannique Halford Mackinder. Pour Spykman (né en 1893 et mort en 1943), la puissance qui contrôlerait le centre de gravité géopolitique et économique de la planète, ce qu'il appelait le *Rimland*, le littoral autour de l'Europe centrale et la Russie, s'imposerait comme la première puissance du monde. Mais leur position géographique confère aux États-Unis un autre avantage qui pendant longtemps a façonné la perception stratégique américaine. Jules Jusserand, ambassadeur de France à Washington de 1902 à 1925, racontait avec beaucoup de malice que les États-Unis étaient bénis parmi les nations car « au Nord, ils avaient un voisin faible, au Sud, un autre voisin faible, à l'Est, du poisson et à l'Ouest aussi ». Pour cette raison, durant la plus grande partie de leur histoire, les États-Unis n'avaient tout simplement pas été confrontés à une sérieuse menace étrangère. À l'exception de la guerre d'Indépendance et de celle de 1812 contre les Anglais, les États-Unis n'ont jamais eu à combattre une grande puissance étrangère sur leur propre territoire pour leur propre défense. Le fait qu'ils aient été longtemps préservés d'un danger extérieur a renforcé un puissant courant isolationniste, même si ce dernier a toujours demeuré l'apanage des préoccupations

sécuritaires et n'a jamais concerné la sphère économique. Mais ironiquement, pour le stratège britannique Colin S. Gray, le « splendide isolement » des États-Unis a créé un lien de parenté avec une tentation unilatéraliste. Le raisonnement, notamment dans son *Maritime Strategy, Geopolitics, and the Defense of the West* (1986), se fonde sur l'idée de l'insularité stratégique du pays, jusqu'à l'avènement de la puissance aérienne véritablement intercontinentale et la longue portée des missiles. Elle a permis aux Américains de faire preuve d'un volontarisme et d'une liberté de décision sans entraves pour s'engager, ou non, dans le monde extérieur à leurs frontières. La contiguïté géographique de la menace n'a pas offert aux nations continentales de l'Europe et de l'Asie la même marge de manœuvre. Donc, la réduction des armes nucléaires, conjuguée avec un bouclier antimissile qui protège le territoire américain ainsi que celui de ses alliés, puisent dans deux tropismes distincts de culture stratégique. L'un d'un ancien sentiment de sécurité conféré par son voisinage faible et son isolement géographique et l'autre d'une projection de sa défense et de ses intérêts sur l'anneau littoral, le Rimland, qui enserrait l'Europe centrale et la Russie mais qui de nos jours se déploie surtout autour de l'Iran et la Chine, malgré les démarches tentées par Washington de traiter positivement ces deux pays.

**

En fin de compte, le traité *New START* comporte deux dispositions qui risquent de tout compromettre. D'un côté, Washington ne voit pas dans cet accord un lien formel entre la réduction des armes stratégiques offensives et la défense antimissile. De l'autre, le droit que les Américains s'octroient de poursuivre toute recherche et développement dans le domaine d'autres types d'armes stratégiques non-nucléaires est récusé par les Russes. Ces derniers soutiennent qu'au contraire le traité interdit précisément les deux. C'est pourquoi, on peut dire à ce jour que ces deux clarifications énoncées par les Américains risquent plutôt d'embrouiller l'entente entre Washington et Moscou ; et l'objectif affiché de *New START* de figurer dans le « *Reset* » des relations risque au contraire de l'enrayer.

Quel avenir pour les DRH d'armée ?

Gaël Kerréneur

Commissaire lieutenant-colonel, stagiaire de la 19^e promotion de l'École de Guerre « Maréchal Juin », ancien officier du corps des bases de l'Armée de l'air dans la spécialité « administration ».

Le *Livre blanc sur la défense et la sécurité nationale* et le processus de révision générale des politiques publiques (RGPP) ont conduit le ministère de la Défense à de profondes mutations. Le processus de réforme engagé a pour objectif de doter le pays d'un outil de défense performant, opérationnel et pérenne dans un contexte budgétaire difficile.

[...]

Ce sont ainsi toutes les fonctions du ministère qui sont passées au crible de la réforme afin de s'attacher à replacer le militaire au cœur de son métier. La rationalisation de l'organisation et l'amélioration des prestations de soutien et d'administration se traduisent par la mise en œuvre d'une chaîne interarmées du soutien, fortement « civilianisée », l'un des leviers de la transformation.

Dans le domaine des ressources humaines (RH), inévitablement au cœur de cette profonde mutation, ce sont d'abord la déflation des effectifs et la « manœuvre » RH associée qui concrétisent l'ampleur de la réorganisation du ministère. Ce sont ainsi 54 000 postes qui sont supprimés au sein du ministère, dont 48 600 pour les seules armées ; le rythme de déflation annuel moyen sur la période de la loi de programmation militaire 2009-2014 est de 8 400 postes. Au-delà de la déflation des effectifs, la traduction la plus significative de la transformation dans la sphère RH réside dans la redistribution des responsabilités.

Les directions des ressources humaines (DRH) d'armée ont vu en quelques années leurs attributions diminuer, notamment au profit de l'état-major des armées (EMA). Ce mouvement semble devoir s'accroître avec la montée en puissance continue de la sous-chefferie RH de l'EMA. Cette prééminence de l'EMA dans le domaine RH n'est qu'une des conséquences des décrets de 2009 qui ont réorganisé le fonctionnement et la gouvernance du ministère ; à tel point que l'on semble se diriger lentement mais sûrement vers une DRH des armées, intégrant en son sein, progressivement et de manière raisonnée, une grande partie des attributions aujourd'hui exercées par les DRH d'armée.

Ce scénario pourrait susciter bien des réticences au sein d'armées fort naturellement attachées à leurs prérogatives. Il n'en est rien, et les hautes autorités de ces armées comme leurs chaînes fonctionnelles RH valident majoritairement cette

évolution vers une DRH des armées forte, propre à renforcer le poids des armées au niveau ministériel. Et un consensus assez large se dégage autour de l'idée d'une DRH des armées plus à même de servir les intérêts des armées dans le domaine RH face à l'ambition de la direction des ressources humaines du ministère de la défense (DRH-MD) du secrétariat général pour l'administration (SGA) de porter les RH du ministère tout entier.

Pour autant, cette DRH des armées ne doit pas représenter une fin en soi. La finalité suprême doit demeurer l'efficacité opérationnelle des forces armées, à laquelle participent aujourd'hui pleinement les DRH d'armée. L'avènement prochain d'une DRH des armées, s'il est inéluctable, paraît aujourd'hui prématuré tant les obstacles à une intégration des DRH d'armée au sein d'une DRH des armées demeurent nombreux. En outre et surtout, les limites à cette intégration doivent être posées et les attributions résiduelles éventuelles des DRH d'armée définies pour que l'avènement annoncé de cette DRH des armées ne compromette pas la capacité des armées de continuer à réaliser leurs missions avec efficacité.

Vers une DRH des armées intégrant progressivement les DRH d'armée ?

Dans le nouveau paysage RH du ministère, le scénario d'une DRH des armées intégrant progressivement tout ou partie des DRH d'armée gagne progressivement les esprits. Les logiques susceptibles de conduire à cette DRH des armées unique sont diverses.

Il peut tout d'abord s'agir d'une évolution décidée à la tête du ministère, dans une démarche de rationalisation toujours plus poussée, que ne peut que favoriser le contexte budgétaire que l'on qualifiera par euphémisme de contraint. La crise de la dette est de nature à inciter dans tous domaines à ne pas excéder la stricte suffisance, et l'éternelle quête de gains d'effectifs peut conduire à considérer comme redondantes une sous-chefferie RH étoffée et des DRH d'armée, et accélérer le passage à une DRH des armées.

Mais cette évolution est également impulsée par l'EMA lui-même ; et l'on a déjà dit que les armées n'y sont pas vraiment hostiles. La transformation dans laquelle s'est lancé le ministère aboutira bientôt à une organisation par métier et non plus par mission. Cette organisation matricielle se prête dans l'absolu à l'existence d'une DRH unique au sein du ministère et la DRH-MD pourrait dans ce cas de figure prétendre à devenir cette DRH du ministère, avec des antennes par armées, directions et services. La stratégie de l'EMA d'une DRH des armées robuste, apte à équilibrer une éventuelle suprématie de la DRH-MD, est ainsi de nature à permettre un partage des responsabilités entre une DRH des armées responsable des RH militaires et une DRH-MD responsable des RH civiles du ministère...

Une autre approche pourrait privilégier une vision « organique », avec un partage de responsabilités entre DRH des armées et DRH-MD fondé sur l'identité

de l'employeur : la DRH des armées serait ainsi responsable des personnels militaires et civils employés au sein des armées. Cette ligne de partage prendrait tout son sens en cas de compétences très techniques ou rares exercées par du personnel civil au sein des armées et pour lesquelles celles-ci devraient être compétentes en matière de RH car elles sont responsables des doctrines d'emploi... Toutefois, cette approche présente de lourds inconvénients sur un plan pratique (statuts différents, mobilité vers et hors des armées, parcours de carrière, etc.) et ne semble en conséquence pas représenter la voie à suivre.

Outre les logiques, le contexte paraît favorable à une intégration progressive, en tout ou partie, des DRH d'armée dans une DRH des armées.

Tout d'abord et comme indiqué *supra*, nombreuses sont les fonctions qui progressivement échappent à la compétence des DRH d'armée.

Ensuite, la transformation a conduit à accroître de manière significative le nombre d'organismes interarmées ; ceux-ci se voient affecter par les armées « pourvoyeuses de compétences » du personnel qui, parfois, ne quittera jamais son organisme d'accueil. Il en est ainsi des agents de restauration, des acheteurs, de certains spécialistes des systèmes d'information et de communication... La tentation est alors naturelle pour les organismes interarmées de créer leur propre DRH. Pour éviter cette dérive, la solution la plus rationnelle pourrait consister à regrouper toutes ces DRH en une seule au niveau de l'EMA, une DRH dont le périmètre serait supérieur à celui des DRH d'armée, et qui aurait naturellement vocation à absorber les plus petites...

Enfin et surtout, la future organisation géographique de la fonction RH reposera sur deux seuls sites : Paris-Balard et Tours. Alors que la DRH de l'Armée de terre et la direction du personnel de la Marine auront rejoint la DRH de l'Armée de l'air à Tours à l'horizon 2013, les principaux échelons de conception et de décision RH interarmées et d'armée seront colocalisés sur le site de Paris-Balard à l'horizon 2015. L'étude relative à la sous-chefferie RH en version Balard, dite CIA (centre interarmées) RH, fait état d'une « certaine plasticité dans les structures » possible grâce à cette colocalisation et des transferts d'effectifs possibles des DRH d'armée vers le CIA RH au gré de l'évolution des attributions de ce dernier. Certes, cette étude affirme aussi que le maintien de la référence à une des trois armées d'appartenance constitue le principe fondamental de la politique et de la gestion du personnel militaire et que les armées et services conservent les attributions RH telles que décrites *supra*.

Mais cette concentration des responsabilités RH des armées sur les sites de Paris et Tours crée indéniablement de manière opportune les conditions favorables à une intégration des DRH d'armée au sein d'une DRH des armées, selon des modalités qu'il convient maintenant de préciser.

Les obstacles à cette intégration

Les obstacles à une création d'une DRH des armées et à une intégration pleine et entière en son sein des DRH d'armée sont de plusieurs ordres. Ensuite, cette évolution n'est pas souhaitable : cette intégration doit donc être partielle, raisonnée, les DRH d'armée devant perdurer et conserver des attributions résiduelles, garantes du maintien de l'efficacité opérationnelle des armées.

Les obstacles à la création d'une DRH des armées absorbant purement et simplement les DRH d'armée sont tout d'abord d'ordre législatif et réglementaire. Le Code de la défense précise qu'un engagement est souscrit « au titre d'une armée », et c'est ainsi que toutes les décisions RH relatives à la progression de carrière depuis le recrutement jusqu'à la radiation des cadres ou des contrôles relèvent de la responsabilité de l'armée d'appartenance. Le décret n° 2009-869 ajoute que les CEM d'armée « sous l'autorité du chef d'état-major des armées (...) assurent la préparation opérationnelle des forces placées sous leur propre autorité ; ils sont responsables, pour leur armée, du recrutement, de la formation initiale, de la discipline, du moral et de la condition des militaires ». Sur un plan budgétaire, les DRH d'armée assurent pour le compte de leur CEM, au titre de responsable de budget opérationnel de programme (RBOP), le pilotage du Titre II. Le caractère structurant de l'organisation budgétaire instaurée par la Loi organique relative aux lois de finances (Lolf) doit une nouvelle fois être souligné ici.

Tout aussi problématique est la satisfaction des conditions d'ordre fonctionnel. La modernisation de la gestion des RH du ministère, menée par la mission SI-RH (relevant de la DRH-MD), passe tout d'abord par la définition de nouveaux processus métiers simplifiés, harmonisés et rationalisés, et par la réalisation du futur Système d'information, de gestion des ressources humaines (SIRH) ministériel unique qui portera ces processus à partir de la fusion et de la convergence des cinq SIRH majeurs existants. Des processus RH harmonisés et un SIRH unique sont un préalable indispensable à la mise en place d'une DRH des armées.

Certes, le déploiement de ce SIRH unique est prévu pour 2014 afin d'être en 2016 au rendez-vous du raccordement à l'ONP, mais ce sont environ 160 processus RH qui ont été recensés dans le ministère et leur harmonisation se révèle extrêmement difficile. Seuls de très rares processus ont été harmonisés à ce jour (ou sont en voie de l'être), les plus emblématiques étant ceux relatifs à la notation. Ceux relatifs au recrutement, à la formation, à l'avancement, à la mobilité notamment, parmi les plus complexes, sont en chantier...

Les échéances annoncées paraissent de fait extrêmement ambitieuses et malgré les efforts consentis, très importants, il est permis de douter qu'elles seront respectées, sauf à risquer une harmonisation « au pas de course » et une dégradation des processus RH actuels. Au-delà de ces obstacles qui ne paraissent en définitive pas insurmontables, il convient de s'interroger sur la pertinence d'une

intégration totale des DRH d'armée au sein d'une DRH des armées, jusqu'à leur suppression, ou sur la nécessité de conserver des DRH d'armée aux périmètres d'activité redéfinis.

De la spécificité des RH militaires

Ce qui doit guider la réflexion, c'est le fait que les RH militaires sont spécifiques en ce qu'elles constituent un outil destiné à préparer la guerre. Il s'agit *in fine* pour les armées, pour chaque armée, de disposer d'hommes et de femmes qualifiés, motivés, aptes à aller au combat pour mener à bien les missions qui leur sont confiées. Et c'est cette spécificité, à la fois vis-à-vis des RH non militaires et propre à chaque armée, qui doit être toujours rappelée face aux tentations de fusionner purement et simplement les DRH d'armée en une seule, voire de penser à une gestion des RH ministérielle ou interministérielle unique.

Les armées se caractérisent par un fort attachement à des valeurs, à une culture. Elles partagent bon nombre de valeurs (discipline, disponibilité...), mais en cultivent également en propre. C'est en effet cette culture spécifique qui est déterminante pour assurer la capacité à mener des actions aux effets stratégiques donnés dans un milieu considéré, et qu'il faut par conséquent impérativement préserver. Par analogie, la culture d'entreprise est considérée en milieu civil comme essentielle, et la mise en place de structures responsables de la gestion RH de plusieurs entreprises est traditionnellement présentée comme pouvant altérer le sentiment d'appartenance à l'entreprise et le lien de rattachement au chef, et au bilan produire une perte d'efficacité...

Les chaînes RH d'armée permettent aux armées de créer leur identité propre, fortifient le sentiment d'appartenance à une armée et de subordination au CEM d'armée ; elles contribuent ainsi au développement des cultures et des compétences de milieu essentielles pour la réalisation des missions assignées aux armées, que celles-ci soient menées de façon autonome ou en milieu interarmées ou international. Ce sont bien les contraintes spécifiques de milieu qui conduisent à la maîtrise de compétences particulières, et ce sont les DRH d'armée par les GPEEC (gestion prévisionnelle des effectifs, des emplois et des compétences) qu'elles mettent en œuvre en relation étroite avec les pôles opérationnels d'armée qui permettent l'acquisition et le maintien de ces compétences.

Bref, l'efficacité opérationnelle des armées paraît incompatible avec une GPEEC centralisée, exercée au sein d'une DRH des armées. L'exercice co-localisé des GPEEC d'armée sous la tutelle de l'EMA, que permet le regroupement des chaînes RH sur les sites de Paris et Tours, favorisera en revanche les synergies.

Quel pourrait être à terme le périmètre d'activité redéfini des DRH d'armée ?

Déchargées de l'élaboration des politiques RH (à l'exception des politiques RH spécifiques), des relations avec les grandes directions du ministère, DRH-MD et directeur des affaires financières (DAF) principalement, et l'extérieur du ministère, les DRH d'armée pourraient schématiquement voir leurs responsabilités recentrées sur la GPEEC de leur milieu – en particulier le pilotage des effectifs du BOP, les flux RH, les politiques de formation propres au milieu – et sur la condition et le moral du personnel « auscultés » grâce au dialogue social.

S'il est des domaines qui doivent impérativement rester dans les périmètres de responsabilité des armées, il en est d'autres qui pourraient encore faire l'objet d'une intégration au sein de la future DRH des armées. Ainsi, à titre d'exemple, la fonction « recrutement » présente des potentialités de mutualisation, sous réserve de préserver la capacité des CEM d'armée à exercer leurs responsabilités en matière de cohérence organique des armées dont ils ont la charge (en laissant par exemple aux armées la responsabilité de la définition de leurs critères de recrutement).

Au bilan, la voie à suivre, avec pragmatisme et sans tabou mais sans dogmatisme, est celle de DRH d'armée aux responsabilités resserrées mais sanctuarisées, liées à la spécificité de milieu et garantes du maintien de l'efficacité opérationnelle des armées.

*
**

Dans le cadre de la transformation engagée au sein du ministère, les RH constituent un enjeu majeur. Les chantiers sont dans ce domaine d'une grande complexité mais ils sont au cœur de la réforme et une des conditions clés de son succès.

Pour que les armées disposent demain en quantité et en qualité, dans un contexte budgétaire extrêmement contraint, de la ressource humaine motivée et qualifiée nécessaire à la réalisation de leurs missions, une réorganisation profonde des RH militaires est indispensable. La création d'une DRH des armées est l'aboutissement inéluctable de cette réorganisation, marquée par la prééminence du Cema et ses responsabilités budgétaires héritées de la Lolf.

C'est là dans le domaine RH toute la difficulté de la transformation lancée au sein du ministère que de conjuguer dans un environnement complexe, parfois hostile, la nécessaire rationalisation de la gestion des RH militaires, la préservation des intérêts des armées et le maintien de leur crédibilité opérationnelle.

L'universalisme occidental : illusion antique ou succès planétaire ?

Nicolas Tenzer

Président d'Initiative pour le développement de l'expertise française à l'international et en Europe (IDEFIE), directeur de la revue *Le Banquet*. Auteur de trois rapports officiels au gouvernement (dont deux sur la stratégie internationale) et de 21 ouvrages dont *Quand la France disparaît du monde* (Paris, Grasset, 2008), *Le monde à l'horizon 2030. La règle et le désordre* (Paris, Perrin, 2011), *La fin du malheur français ?* (Paris, Stock, 2011) et *La France a besoin des autres* (Paris, Plon, 2012).

L'idée d'universalisme nécessairement perçue comme occidentale du fait de son origine fait l'objet d'appréciations contrastées. D'un côté, elle ne peut que paraître inacceptable aux dirigeants et peuples non occidentaux qui insistent sur leur voie particulière de développement et leurs spécificités culturelles. De l'autre, pour qui observe de près les évolutions du monde, la réalité est bien celle d'un processus d'universalisation tout autant que de globalisation. Toutefois, cet universalisme est plus constaté dans certaines revendications – démocratisation, droits de l'homme et parfois de la femme – et formes spontanées d'insurrection, qu'il n'est pleinement assumé. L'élément majeur est que ces aspirations paraissent dictées par la conscience individuelle plus qu'elles ne sont téléguidées par une organisation « communautaire ». Cet universalisme ne paraît pas puiser dans des racines culturelles mais semble issu d'un fonds anthropologique qui est comme révélé par la dynamique sociale et politique. Il exprime quelque chose de brut et d'immédiat qui n'est pas théorisé de façon politique, voire paraît opposé aux « mentalités » de certaines des sociétés où il est apparu. Il est pourtant le signe d'un vacillement du monde où, comme souvent, la manifestation précède la doctrine et l'événement la prise de conscience de celui-ci par ceux qui en ont été les acteurs.

Un ordre international plus commun ?

Si l'on parcourt le monde, on ne peut qu'être frappé par quatre dimensions d'universalisation qui ne signifient pas qu'il existe un universalisme au sens philosophique du terme. Elles sont relativement récentes et indiquent en cela des mutations à l'œuvre. Nous devons, dans un premier temps, en rester aux perceptions qui nous fournissent des indications précieuses sur la marche du monde.

Le premier de ces éléments est le renforcement de la communauté de pensée, la proximité des concepts utilisés et la meilleure compréhension mutuelle entre des personnes venant d'aires géographiques différentes. Il existe souvent plus de

communauté et d'échanges entre des individus qui travaillent sur des sujets communs qu'avec certains de nos compatriotes qui, soit ne partagent pas les mêmes intérêts, soit, les partageant, sont moins internationalisés. Certes, cela ne veut dire ni accord ni absence de concurrence. Cela ne signifie pas non plus que la détermination des finalités liée à une certaine façon de définir les intérêts n'ait pas des racines puisant dans l'histoire et la culture du pays – il faudra le comprendre en particulier lorsqu'il s'agira de négocier. Mais même sur ce point, les codes de traduction sont désormais plus aisés à trouver.

La deuxième évolution, qui explique la première, est celle des élites, y compris de pays qui sont loin d'être des démocraties telles que nous les concevons en Occident. Alors qu'il y a une vingtaine d'années, ces élites – politiques, administratives, intellectuelles, du monde des affaires – généralement peu internationalisées, étaient essentiellement immergées dans des réseaux locaux dont elles ne sortaient pas et utilisaient surtout des stéréotypes pour parler à des étrangers, cette réalité n'est plus le lot commun, sauf dans quelques pays encore coupés du monde. Dans des pays non démocratiques mais pour autant non figés, ces élites qui doivent être capables d'un double ou triple jeu font preuve d'une agilité souvent supérieure aux élites occidentales, précisément parce qu'elles ont dû accomplir un effort considérable pour à la fois rester dans le système et pour en sortir.

Plus importante encore apparaît l'évolution des peuples, troisième clé. Quelque chose comme une conscience liée à la personne apparaît dans bien des révoltes ou insurrections contemporaines, non seulement celles synthétisées sous l'appellation de « Printemps arabe », mais aussi dans d'autres zones du monde – en Asie, en Asie centrale, en Afrique subsaharienne, sans même évoquer l'Amérique latine, évidemment plus occidentalisée. Si certains individus ont certes été utilisés et récupérés par des mouvements communautaires et religieux, une certaine forme de spontanéité dans ces mouvements montre qu'on est de plus en plus infondé à décrire ces sociétés comme marquées par des formes d'appartenance « holistes ». Sans pouvoir faire droit à l'idée d'une occidentalisation de la conscience, cela conduit pour le moins à rejeter la notion de civilisation ou même de culture, même s'il en existe naturellement des traits spécifiques, en termes notamment de réseaux de socialisation. Nous pouvons faire l'hypothèse que la volonté d'émancipation politique transcende les différences culturelles ou religieuses, voire même que l'idéologie, la culture et la religion joueront un rôle moins dominant dans les comportements politiques qu'ils ne le paraissent. Elles continueront certes à le faire pendant un certain temps, notamment en raison de la force des islams dans plusieurs pays, mais cela tiendra plus à la puissance sociale et politique de certains groupes qu'à une adhésion entière, indépendante des aspirations à la liberté et de la résistance à l'oppression.

La quatrième nouveauté tient à ce qu'au sein d'un monde où il existera simultanément plus de compétition et de concurrence d'un côté mais aussi plus de capacités de dialogue de l'autre, on assistera au renforcement des stratégies étatiques ou nationales liées à la maturité accrue des élites, voire des peuples. Ce renforcement

se fera vraisemblablement sans affirmation accrue d'un nationalisme, sauf peut-être paradoxalement en Europe et dans certaines zones du monde. Là aussi, le facteur politique sera premier par rapport à l'arrimage des populations à des sentiments « archaïques » d'appartenance. La fierté nationale passera par une certaine forme de modernisation des États.

Malaise dans l'universalisme occidental

Par un surprenant paradoxe, alors même que plusieurs pays font un chemin vers l'universalisme, certaines sociétés occidentales semblent emprunter la trajectoire inverse. Pour aller vite, le projet de l'universalisme était historiquement lié aux Lumières et fondé sur l'idée d'émancipation. Pour des raisons politiques, sociales et philosophiques, ce projet d'émancipation explicite – qu'est une personne émancipée et, en particulier, que cela suppose-t-il en matière d'éducation ? – a disparu de nombreux projets politiques. Alors même que le projet d'universalisme dans la plupart des pays passe par une autonomie accrue de la sphère publique par rapport à la religion, le principe strict de laïcité est remis en cause par certains groupes de pensée en Occident. Au demeurant, il n'est pas reconnu comme principe cardinal par certains pays occidentaux. Celui-ci peine aussi de plus en plus à exprimer des valeurs liées à cette émancipation.

S'y ajoute le fait que, alors que les progrès de l'universalisme viennent de l'ouverture au monde d'une partie, certes encore limitée, de sociétés jadis fermées, on voit poindre à l'Ouest des menaces sur l'ouverture de nos sociétés, alors qu'ouverture économique, ouverture des frontières et ouverture intellectuelle vont de pair.

Le monde occidental a aussi abandonné toute réflexion sur les dangers d'asservissement qui proviennent de la société – ce qui était déjà un avertissement de Tocqueville – et souvent menacent plus l'individu que ne le fait l'État. C'est d'ailleurs l'un des principaux défis que connaissent aussi la plupart des sociétés qui s'essayent à la démocratie : une fois le danger d'oppression par l'État éliminé ou amoindri, comment agir pour que ne se renforcent pas les menaces qui proviennent des groupes sociaux, qu'ils soient communautaires, claniques ou religieux ?

Universalisme et émancipation

En arrière-plan des évolutions vers une forme d'émancipation de nombreuses sociétés, il existe des questions philosophiques dont la résonance politique est évidente.

La première est directement liée à l'universalisme. Pour le comprendre, il convient d'écarter deux idées. La première est d'ordre moral et voudrait que ce qui est universel soit *a priori* meilleur et supérieur à ce qui ne l'est pas. Outre que cette idée n'est pas démontrable, elle introduit une forme de pression qui ne peut que susciter le rejet. La seconde résiderait dans l'affirmation d'une vérité : l'universalisme

serait plus vrai que le particularisme. Des raisons analogues conduisent à écarter cette présupposition. Il devient dès lors possible de traiter de l'universalisme de manière pragmatique, ce qui suppose non de se demander s'il existe un état supérieur de la conscience à « rejoindre » selon une méthode qui consisterait à miner le processus qui s'est accompli en plusieurs siècles en Occident mais de vérifier le constat suivant : est-il vrai que de plus en plus de peuples finissent, sur des sujets liés aux libertés et aux droits, par adopter des attitudes similaires indépendamment de leur territoire d'origine ? Dès lors, l'« occidentalisme » de l'idée d'universel devient une question relativement secondaire. Certes, historiquement, les principes de ce qui apparaît aujourd'hui de plus en plus universellement partagé sont bien nés en Occident mais ce n'est pas une pression « impérialiste » qui a fait naître les aspirations à la liberté, à la démocratie et à la reconnaissance des droits, d'autant qu'on retrouve celles-ci chez des gens qui n'ont pas étudié la philosophie classique et n'ont été que peu en contact avec l'Occident. Si ces personnes ont bien repris, quoique parfois de manière sélective, certains des modes de vie de l'Ouest, ceux-ci n'ont eu qu'un effet indirect sur l'émergence de leurs revendications. En tout cas, il n'est pas possible d'affirmer qu'il y aurait, par nature, des cultures où ces idées ne pourraient trouver place. L'aspiration à la liberté relève en cela d'une anthropologie qui se réveille quand les conditions sociopolitiques l'autorisent.

Cette question appelle l'examen d'une seconde : celle de la civilisation. Sans doute historiquement peut-on affirmer qu'il existe bien des civilisations – occidentale, chinoise, indienne, arabe, etc. Mais ces civilisations ne sont ni closes ni homogènes, comme le montre l'analyse sociologique. La géopolitique révèle à son tour que de nombreux pays cherchent aujourd'hui, pour des raisons stratégiques, des alliances plus fortes avec des pays plus lointains, quoique moins proches culturellement, bien plus qu'avec leurs voisins. Les différents pays sont plutôt enclins à combiner ce qui reste de leur culture avec d'autres apports, pour des raisons politiques, et l'on peut parfaitement concevoir, par exemple, que des « valeurs asiatiques » plus attentives aux éléments de cohésion de la communauté, y compris par le travail orienté vers celle-ci, puissent se conjuguer avec l'irruption de la conscience et des droits individuels. Aucune société n'évolue de manière linéaire et la forme d'universalisme dont on voit poindre l'émergence n'est aucunement un développementalisme.

Reste une troisième question, qu'il convient aussi de traiter de manière pragmatique et non normative : celle de la différence. Jusqu'où est-elle possible et acceptable, tant dans l'ordre interne que dans l'ordre international ? Quelle mesure les gouvernements doivent-ils trouver entre l'excès de différence, qui rend la communication et la pacification impossibles, et le rejet absolu du différent, qui entraîne toujours le conflit et la fermeture des nations et des esprits ? Ni l'angélisme du dialogue qualifié parfois de « dialogue entre les civilisations » qui, involontairement, légitime leur clôture, ni le bellicisme de la séparation ne sont acceptables et ne correspondent aux espoirs que l'universalisme a suscités.

L'universalisme dans notre agenda politique international

L'évolution du monde dans le sens de cette universalisation oblige à adapter notre politique internationale, à la fois quant à la méthode et sur le fond. Elle conduit également à mesurer ses implications dans l'ordre interne.

Sur la méthode, nous devons prendre au sérieux le souci de développer les échanges intellectuels avec des nouveaux pays qui effectuent un effort substantiel pour être eux-mêmes présents dans les lieux internationaux de débats, organisent des séminaires et multiplient *think tanks* et universités. Disons-le clairement : nous devons être à la hauteur et ne pouvons pas faire moins. Nous devons aller les voir, discuter, comprendre leurs intérêts et leur stratégie, leur apporter aussi la contradiction, produire autant qu'eux. C'est un plan de présence à l'international que nous devons développer. Notre diplomatie doit aussi s'employer à mieux connaître les différentes sociétés ; nos ambassades doivent être toujours plus des espaces ouverts, permettant d'explorer les lieux les plus larges et de repérer les forces qui, demain, seront motrices.

Sur le fond, le mouvement d'universalisation n'est pas continu mais heurté. S'il ne tolère point que les pays occidentaux se posent en consciences morales infaillibles, il doit être aussi accompagné. Mais ce soutien se fait aussi dans un contexte de concurrence accrue, parfois de quasi-guerre froide, des règles, des normes et des bonnes pratiques. Nous avons des principes à défendre et, pour ce faire, nous devons être présents, apporter de la contre-expertise aux expertises douteuses et devons forger plus explicitement nos idéaux conformément à un projet d'émancipation. Quasiment tous les domaines sont concernés : il ne faut pas seulement considérer la « superstructure » (les droits de l'homme et les libertés civiles) mais aussi l'« infrastructure » (la bonne gouvernance, l'agriculture, l'éducation, le développement durable, l'action des services de police). Ce sont aussi les conditions de développement, les rapports sociaux et la gestion des hommes qui font que ce processus d'universalisation peut se prolonger dans la durée. Bien sûr, nous devons être totalement fermes sur la question des droits humains. Le message doit être envoyé aux États, sans ambiguïté mais aussi sans prétention de supériorité ; il doit l'être tout autant à l'égard des groupes sociaux. Cela passe d'abord par le refus de tout discours fondé sur le « différentialisme » qui correspondra de moins en moins à la réalité. Nous devons nous présenter systématiquement du côté des forces d'émancipation, tout en prenant en compte le potentiel de démocratisation des différentes sociétés.

En Europe en particulier, nous devons avoir une définition puis une action plus claires de promotion de nos valeurs partagées et lutter contre leur transgression, d'abord chez nous. Nous devons ensuite communiquer sur ce message de l'Europe au monde, y compris par les programmes de coopération technique et pas seulement par des déclarations politiques.

Dans l'ordre intérieur, outre le renforcement chez nous de la connaissance du monde par l'éducation – en histoire, géographie et littérature notamment – et des événements mondiaux du dernier siècle, nous devons être plus fermes à la fois sur nos valeurs et sur l'exigence d'ouverture de nos sociétés, les deux allant de pair. Sans doute, devons-nous aussi comprendre que ce qui va rendre potentiellement, s'il réussit le processus d'universalisation, si fort ailleurs, c'est qu'il s'accompagne de modes d'être en société plus communautaires que chez nous. Peut-être est-ce ainsi que nous devons à notre tour revisiter le processus d'universalisation, en redécouvrant à la fois ce qui nous est commun – en somme le patriotisme classique – et l'importance du processus de désaliénation de la personne – ce qu'on pourrait appeler le « bon » individualisme – par rapport au conformisme social, qui n'est producteur ni de liens ni de valeurs. En somme, il s'agit de mettre ensemble les principes et les valeurs qui tiennent une communauté (et cela vaut particulièrement en Europe), l'autonomie individuelle (autrement dit la distance critique, y compris par rapport à sa propre histoire) et l'ouverture internationale et la multitude d'échanges qu'elle autorise et suscite.

Le processus d'universalisation des autres est une forte incitation à réfléchir sur l'exemplarité de l'Occident.



■ ***Revue - Rapports - Recensions***

RDN

Revue Défense Nationale - Juin 2012

ANALYSE STRATÉGIQUE

La Chaire Castex de cyberstratégie

Sur la base d'une convention de mécénat entre le Cercle des partenaires de l'IHEDN et la Fondation d'entreprise d'EADS, la Chaire Castex de cyberstratégie a été créée en novembre 2011. Organe de réflexion sur l'action dans la « cinquième dimension », la 5D, elle sensibilise les acteurs de la société civile dans tous les secteurs d'activités et à tous les niveaux de responsabilité et de décision.

Elle favorise le développement de la recherche dans le monde universitaire français et encourage les coopérations académiques extérieures. Elle contribue à l'approfondissement du dialogue international à des fins de coopération et de compréhension mutuelle.

Fondements

Le cyberspace forme l'univers virtuel au sein duquel circule l'information numérique. Mais en inférant que le cyberspace est purement immatériel, on commettrait un contre-sens. La 5D repose sur une infrastructure technique matérielle faite de machines, de câbles, de nœuds de transmission, physiquement localisés et sur une superstructure que nous nommons « cyberarchie », composée des différentes catégories d'opérateurs qui l'orientent, la financent et l'organisent en fonction d'objectifs et d'intérêts généraux et particuliers.

Le cyberspace constitue aujourd'hui un domaine stratégique à part entière en raison de son fonctionnement organique. Il est aussi intrinsèquement lié aux autres domaines de l'action humaine civile et militaire, publique et privée. S'y jouent la prospérité des entreprises et la richesse des

nations. Devenue en quelques années un théâtre d'affrontements internationaux, la 5D s'érige en objet stratégique, qui doit être pensé dans toutes ses composantes et selon les différents modes d'action défensif, offensif, dissuasif.

En raison de la diversité terminologique (protection, sécurité, défense) qui ne couvre pas l'intégralité du champ des activités du cyberspace, nous avons adopté le concept englobant de cyberstratégie : « ensemble des pratiques civiles et militaires, publiques et privées, intérieures et extérieures visant à aménager et à utiliser le cyberspace afin de répondre aux objectifs fixés par l'autorité politique pour assurer la prospérité et la sécurité de la communauté des citoyens, en conformité avec les impératifs de souveraineté et d'autonomie de décision nationales, dans le respect des libertés matérielles (économie) et spirituelles (idéologie) ».

Centrée sur la géopolitique et la géostratégie de la « cinquième dimension », la Chaire n'a pas vocation à mener des études techniques. Pour garantir la fiabilité des analyses, elle dispose d'une équipe d'experts en sécurité des systèmes d'information.

Six domaines d'études sont distingués

1. L'approche géopolitique du cyberspace se fonde sur l'analyse comparative des concepts et des doctrines d'emploi des grands acteurs mondiaux et leurs évaluations croisées de la menace.

2. Ce domaine est complété par l'étude des acteurs étatiques et infra-étatiques à l'échelle régionale. Ceci permet d'engager l'analyse des catégories et des formes de la contestation politique et du cyberterrorisme. Dans ce dernier cas, on évalue les agressions visant à détruire des infrastructures critiques pour provoquer de graves dommages physiques et psychologiques.

3. L'analyse des menaces et des vulnérabilités majeures et la recherche sur les contre-mesures se concentre sur les opérateurs d'infrastructures critiques. On conduit une analyse des acteurs, des menaces (armes, procédés, intentions), des tactiques, des cibles et des vulnérabilités : attaques sur la racine du DNS, sur le routage, etc. On s'attache aux agressions les plus remarquables, soit en termes de sophistication de l'attaque, soit en termes de défaillance majeure de la protection, soit les deux à la fois. Quelles pourraient être les nouvelles vulnérabilités et les nouvelles malveillances compte tenu de l'évolution rapide des technologies ? Quelle protection apporteront les nouvelles capacités cryptologiques ?

4. Une étude de l'économie politique du cyberspace est nécessaire. La Chaire s'emploie à mesurer le coût direct des agressions comportant les pertes financières dues aux attaques, en la complétant par l'évaluation des coûts indirects incluant la détérioration d'image et de confiance auprès des consommateurs. On recherche aussi les composantes majeures d'une politique industrielle en matière de cybersécurité tant au niveau de la France qu'au sein de l'Union européenne dans son ensemble. L'enjeu consiste à analyser, à suivre mais aussi à inspirer des principes susceptibles de présider à la structuration d'un marché de la cybersécurité.

5. La cyberdiplomatie et le droit international sont à étudier conjointement. Ce domaine concerne les propositions de législation aux Nations unies faites par différents

États et les offres de dialogue bilatéral, avec ou sans conditions préalables. Est-il envisageable et souhaitable de s'engager dans la voie d'une maîtrise des armements ? Peut-on se contenter d'accords de bonne conduite et de normes de comportement coopératif en se dispensant de dispositions à valeur universelle ? On examine aussi les discussions, concertations et les accords au sein des différentes organisations internationales (UE, Otan, Organisation de coopération de Shanghai). En quoi ces formations sont-elles affectées par l'usage du cyberspace en regard de la souveraineté et de l'autonomie de chaque État-membre ?

6. Éthique et sécurité humaine dans l'âge de l'information. On suit l'élaboration des dispositions réglementaires relevant des actions menées au niveau européen pour établir les règles de bon comportement des gouvernements et des citoyens. Celle-ci relève, en effet, d'une politique communautaire qui ne peut s'affranchir de principes et d'intérêts relevant de la souveraineté de chaque État, conformément à sa culture et à ses institutions. Les idéologies politiques et religieuses sont concernées car le cyberspace est devenu un domaine de confrontation des cultures.

Dans chacun de ces domaines, la Chaire se veut une force d'analyse, d'innovation et de proposition.

François Géré

*Stratégiste, président de l'Ifas,
Titulaire de la Chaire Castex de cyberstratégie
(www.cyberstrategie.org)*

CENTRE INTERARMÉES DE CONCEPTS, DE DOCTRINES ET D'EXPÉRIMENTATIONS

Travaux de concept
et de doctrine de cyberdéfense

Les systèmes d'information sont devenus presque indispensables au fonctionnement

même de nos sociétés modernes. Parallèlement, le développement rapide des réseaux informatiques et d'*Internet* a révolutionné la plupart des activités, y compris celles de l'État. Si cela a procuré des gains de productivité, d'efficacité et de confort considérables, cette nouvelle dépendance nous place aussi dans une situation inédite de

vulnérabilité et le cyberspace est devenu un lieu d'affrontement.

C'est le constat fait dans le *Livre blanc sur la défense et la sécurité nationale* qui, en 2008, souligne la nécessité d'adapter notre stratégie aux nouveaux risques et aux nouvelles menaces liés au cyberspace en se dotant des organisations et des moyens permettant d'y faire face et d'agir.

C'est ainsi que l'Agence nationale de sécurité des systèmes d'information (ANSSI) est devenue autorité nationale de défense des systèmes d'information et qu'une stratégie nationale en matière de défense et de sécurité des systèmes d'information a été adoptée.

En cohérence avec cette organisation gouvernementale, le ministre de la Défense a confié la responsabilité de la défense des systèmes d'information du ministère et des armées au Chef d'état-major des armées, qui a mis en place une structure dédiée à la cyberdéfense. Dans ce cadre, ont été publiés, respectivement en juillet 2011 et janvier 2012, un concept puis une doctrine interarmées de cyberdéfense consacrés aux aspects défensifs du domaine.

Le concept définit le cadre général dans lequel se situe la cyberdéfense pour l'ensemble du ministère, donne les fondements et les principes de son efficacité puis en déduit les grandes aptitudes qu'elle requiert.

La doctrine détaille, à partir de ces aptitudes, les fonctions et moyens de la cyberdéfense, décrit l'engagement et précise les responsabilités respectives de l'état-major des armées, des opérateurs de systèmes d'information, des armées, des directions et services du ministère en matière de cyber-défense.

La cyberdéfense recouvre l'ensemble des activités conduites dans le cyberspace pour garantir l'efficacité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère. Elle s'appuie naturellement sur les mesures de

protection des systèmes d'information, mises en œuvre par la chaîne fonctionnelle de sécurité des systèmes d'information, et les complète. L'objectif est de passer d'une défense passive à une défense active en profondeur, doublée d'une capacité de gestion de crise cybernétique et d'une capacité de conduite d'opérations dans le cyberspace.

Dans sa mise en œuvre, la cyberdéfense nécessite d'abord de connaître le cyberspace et d'anticiper les risques et les menaces. Les technologies de l'information étant en perpétuelle et rapide évolution, il est indispensable d'acquérir et d'entretenir une connaissance approfondie du domaine. Pour cela, les compétences propres des armées et du ministère doivent s'appuyer, avec l'ANSSI, sur des collaborations avec l'industrie et le monde de la recherche comme sur des coopérations avec nos principaux partenaires, notamment au sein de l'Otan. Parallèlement, une parfaite connaissance de nos systèmes et de leurs fonctionnalités comme des procédures d'utilisation doit permettre de mieux analyser nos vulnérabilités. Des travaux de planification opérationnelle doivent aussi être conduits et des plans de cyberdéfense établis pour prendre en compte les risques et les menaces et préparer les réponses appropriées.

Il faut, en second lieu, entretenir une veille permanente des systèmes et des réseaux, fondée sur des moyens techniques, des spécialistes, et les utilisateurs eux-mêmes, pour détecter au plus tôt toute anomalie puis l'analyser. Des mesures adaptées pourront ensuite être prises pour résoudre l'incident et réagir s'il s'agit d'une attaque. Cette veille permanente et la connaissance du milieu permettent d'entretenir une situation cybernétique à partir de laquelle une posture de cyberdéfense est définie.

Il faut enfin disposer d'une capacité de commandement et des outils nécessaires – organisation, procédures, matériels, équipes spécialisées – pour se défendre, gérer une

crise cybernétique, évaluer les conséquences opérationnelles et restaurer les systèmes affectés.

Une chaîne de commandement interarmées et ministérielle unique a donc été mise en place pour organiser et conduire la défense des systèmes d'information du ministère selon ces principes. Une haute autorité de cyberdéfense a été désignée. Sa responsabilité est à la fois opérationnelle, pour la coordination et la conduite des opérations de défense des systèmes d'information du ministère, et transversale pour animer et coordonner les travaux relatifs au domaine de la cyberdéfense et à sa montée en puissance.

La structure de cyberdéfense en place au niveau central se développe rapidement pour irriguer l'ensemble des armées, directions et services avec des organisations adaptées, des procédures rôdées, des spécialistes formés, des utilisateurs informés et du matériel adapté.

Le tournant de la cyberdéfense a été pris et elle monte en puissance. Son efficacité sera évaluée à l'aune des attaques régulières dont les systèmes d'information du ministère sont la cible et à partir d'exercices spécifiques ou d'exercices sur d'autres thèmes auxquels seront inclus des événements de cyberdéfense.

CV Sébastien Gourtay

PARMI LES LIVRES

Marins, explorateurs, roman maritime ⁽¹⁾

« Il y a dans la vie du marin quelque chose d'aventureux qui nous plaît et qui nous attache. Ce passage continu du calme à l'orage, ce changement rapide des terres et des cieux, tiennent éveillée l'imagination du navigateur. Il est lui-même, dans ses destinées, l'image de l'homme ici-bas : toujours se promettant de rester au port et toujours déployant ses voiles ; cherchant des îles enchantées où il n'arrive presque jamais, et dans lesquelles il s'ennuie s'il y touche ; ne parlant que de repos et n'aimant que les tempêtes ; périssant au milieu d'un naufrage ou mourant vieux rocher sur la rive, inconnu

des jeunes navigateurs dont il regrette de ne pouvoir suivre le vaisseau » (Chateaubriand).

Cet exergue peut suffire à lui seul à justifier l'existence d'un genre littéraire et philosophique, celui du voyage, de l'aventure, du départ, de la découverte des autres et de soi. Malraux disait que l'on voyageait pour des raisons sexuelles, peut-être, si l'amour est entendu dans son sens véritable, d'*éros*, de *philia* et d'*agapé*. À l'heure du monde fini, l'ailleurs continue sinon de fasciner, au moins de nous interroger, preuve que la Terre n'est pas aussi plate qu'on a voulu le croire.

• Producteur-animateur (*Mauvais Genres*) et chroniqueur à *France-Culture* – on lui doit notamment chez le même éditeur un dictionnaire Jules Verne – François Angelier a choisi, pour rédiger son copieux dictionnaire, des bornes chronologiques fort larges allant des invasions mongoles du XIII^e siècle au cataclysme nucléaire du XX^e. Grâce à lui, le lecteur redécouvre les figures classiques du voyage et de l'exploration comme Marco Polo, Christophe Colomb, James Cook, Roos, Charcot, Amundsen, sans compter les figures incontrôlables comme Alexandra David-Néel. Il lui a fallu opérer un savant

(1) Cf. François Angelier : *Dictionnaire des Voyageurs et Explorateurs occidentaux du XIII^e au XX^e siècle* ; Pygmalion, 2011, 766 pages. Étienne Taillemite : *Bougainville* ; Perrin, 2011. Claire Laux : *Le Pacifique aux XVIII^e et XIX^e siècles une confrontation franco-britannique enjeu colonial et rivalité géopolitique* ; Khartala, 2011, 334 pages. Odile Gannier : *Le Roman maritime - Émergence d'un genre en Occident* ; Presses de l'université Paris-Sorbonne, 2011, 612 pages. Vincent Guigueno : *Les phares, gardiens des côtes de France* ; Découvertes Gallimard, 2012, 128 pages.

dosage entre les nationalistes, les époques, les types d'explorateurs et de voyageurs car qu'y a-t-il de commun entre pères dominicains, maristes ou *conquistadors* espagnols, amiraux anglais, coupeurs de bois canadiens, trappeurs et chercheurs d'or ? Mais aussi diplomates italiens, russes, nombreux géophages allemands, botanistes, alpinistes, corsaires de tout poil. De Mathias Abad, missionnaire dominicain qui explora la Colombie au XVII^e siècle à Heinrich Zollinger, botaniste et explorateur suisse du XIX^e siècle qui s'est rendu à Java et aux îles de la Sonde, on le voit, la liste est longue, variée, foisonnante. De fait, on en apprend autant sur les contrées découvertes, explorées, visitées, cartographiées et décrites que sur les hommes (pourquoi si peu de femmes ?) et leurs motivations aussi variées que les passions et les valeurs humaines.

- Type même du navigateur des Lumières par sa culture scientifique, son goût pour les mathématiques (*Traité du calcul intégral*, 1749-1756) son ouverture d'esprit, son insatiable curiosité pour les choses, les hommes et les lieux les plus divers, Louis Antoine, comte de Bougainville est un des rares marins français dont le nom a survécu dans la mémoire collective. On sait qu'il a donné son nom à une île de Papouasie-Nouvelle-Guinée, la plus grande des îles Salomon, ainsi qu'à une fleur. Ses seuls titres de gloire auraient suffi à l'inscrire au Panthéon de la pensée. Mais c'est surtout sa longue et forte variée carrière qui force l'admiration. Tour à tour officier de l'Armée de terre, mathématicien, diplomate, combattant, ethnographe fort intéressé d'abord par les Indiens du Canada, où il accompagna Montcalm, en 1756, puis marin explorateur, philosophe, puis de nouveau combattant sur mer cette fois-ci pendant la guerre d'Amérique ; enfin, pour couronner ce brillantissime parcours savant, il devient membre de l'Académie de marine et des sciences puis de l'Institut ; ce qui illustre la richesse de son parcours dont tous les éléments se soutiennent et se complètent. La

relation de son voyage autour du monde, effectué de 1766 à 1769, publiée en 1771 lui assura un large succès. Bougainville mourra à quatre-vingt-deux ans couvert d'honneurs et sera inhumé au Panthéon.

- Maître de conférence en histoire contemporaine à l'université de Bordeaux III et chargée de cours d'histoire moderne à l'Institut catholique de Paris, Claire Laux a effectué un travail remarquable qui, bien qu'essentiellement historique, jette des lumières sur le Grand océan. Sa belle introduction offre en effet un tableau des plus complets du Pacifique, tel qu'il demeure encore dans notre conscience collective. Un bout du monde, resté si longtemps inaccessible, auréolé de dix mystères, réceptacle de tant de phantasmes de l'homme européen se sentant corrompu par la civilisation. Elle replace l'histoire du Pacifique, non dans la longue durée mais depuis l'établissement de la *pax Britannica*, permise par l'ouverture du canal de Suez en 1869 et l'arrivée des premiers missionnaires de la *London Missionary Society*. Tyrannie des distances, il fallait encore quinze jours au XIX^e siècle pour passer de Tahiti à Hawaï, formant deux des pôles du triangle polynésien. Elle n'oublie pas de mentionner les potentialités économiques des îles du Pacifique assez inégales d'ailleurs car, en dehors de quelques sites miniers, les principales d'entre elles ne sont constituées que des produits de la mer, fruits et plantes exotiques. Cette histoire du Pacifique perçu sous l'angle de la rivalité séculaire franco-britannique est scandée par différentes périodes. Celle de 1820 à 1840 de l'exploration qui achève l'œuvre des grands navigateurs, aux premiers rangs desquels l'inégalable James Cook. De 1880 à 1914, on passe du Pacifique des Lumières à celui des baleiniers, si bien décrits par Melville, des marins, des trafics mais aussi des missionnaires, présents dès 1797, et qui ont fortement marqué les esprits. On s'en rend compte aujourd'hui par l'intense religiosité des habitants, la profondeur de leur foi.

Certes, le Pacifique Nord fut d'abord essentiellement espagnol, ce fut le fameux galion de Manille et l'on en perçoit bien des traces à Guam, aux Mariannes ou en Micronésie, au moins jusqu'à la défaite de l'Espagne face aux États-Unis en 1898. Mais le Pacifique Sud, le plus dense, le plus couvert d'îles fut celui de la domination britannique hormis la présence française à Tahiti, en Nouvelle-Calédonie et à Wallis et Futuna, si l'on met à part le cas du *condominium* des Nouvelles Hébrides. Cette histoire de la rivalité franco-britannique, se révèle une véritable histoire du Pacifique lui-même, tant elle en recouvre les multiples aspects. Celui du glissement des mythes à la découverte, de la découverte aux mythes, des géographies réelles et rêvées, des récits de voyages des missions, des îles escales, des trafics insalubres, des nouveaux enjeux jusqu'aux économusées. Les îles sont autant de points nodaux du renseignement. Peu à peu, les influences politiques et les retombées de la suprématie britannique sur le Grand océan se sont fait sentir, résultat de sa mainmise sur les grandes routes maritimes du globe. Un des éléments du succès britannique, parmi d'autres, fut que le Royaume-Uni disposa plus tôt d'horloges marines plus précises. Ces mondes, encore méconnus, firent l'objet d'une approche de plus en plus scientifique. Les rivalités franco-britanniques s'exacerbèrent notamment à propos de la Nouvelle-Zélande où Dufresne trouva la mort dans un affrontement avec les Maoris. La décennie 1870-1880 vit l'exacerbation de ces rivalités. Après sa défaite, face à la Prusse, la France organisa la colonisation à marche forcée de la Nouvelle-Calédonie en y envoyant les ex-Communards (Louise Michel, Rochefort). En 1880, la Grande-Bretagne et la France ont mis en place des modes d'exploitation et de relations avec les peuples très différents. Ce fut aussi la fin du partage, avant la grande vague des annexions (1884-1900) puis l'entente, singulier compromis, qui devient cordiale dans le Pacifique avec le

condominium des Nouvelles-Hébrides. Mais déjà à la fin du XIX^e siècle, on assiste à la montée en puissance des nouveaux acteurs, États-Unis, Allemagne wilhelmiennne, Japon, ce dernier ayant racheté certaines colonies espagnoles.

Un ouvrage dense et complet qui s'étend sur de nombreux sujets. Celui de la colonisation économique, de la naissance d'un multiculturalisme, celui de l'Océanie des phosphates à Nauru, du guano, du nickel de la Nouvelle-Calédonie, du cuivre de Bougainville.

Un riche glossaire, une volumineuse bibliographie clôturent son livre qui abonde en trouvailles comme cette citation de Victor Hugo à propos du navire à vapeur : « Une mécanique bonne à pas grand-chose ». Décidément après les « arpents de neige » de Voltaire, nos grands écrivains n'auront guère été lucides en géopolitique surtout à l'égard de la Grande-Bretagne ! Autre particularité plutôt française : plus l'Océanie originelle disparaît, plus les artistes s'emploient à la recréer et la façonner à leur goût ou leur imagination. Ce fut l'œuvre des expositions, des géographes et des littéraires, nostalgies d'artistes de Paul Gauguin à Victor Segalen. Le Pacifique insulaire a fourni des terrains d'épanouissement de l'anthologie, sans parler de son impact sur l'art moderne, par le truchement de l'Allemagne du mouvement *die Brücke*, sans parler de Gauguin.

• Normalienne, agrégée de lettres, professeuse de littérature générale et comparée à l'Université de Nice-Sophia Antipolis, Odile Gannier explore avec une rare profondeur ce genre littéraire spécifique qu'est le « roman maritime ». Son existence, même s'il est apparu plutôt tardivement comme une catégorie à part, ne saurait être niée. Joseph Conrad, pour ne citer que lui, relève que rares sont les espaces qui renvoient d'aussi puissants échos exprimant la complexité du lien entre l'homme et la mer, liens amplifiés par le truchement de l'écriture. La polysémie « fortune de mer » est l'occasion de

s'interroger sur ce que la mer n'a cessé de représenter pour l'homme. Est-ce de la chance, de la réussite, une destinée ? Très tôt l'homme a raconté la mer. Ulysse, le héros le plus humain, le premier personnage romanesque, n'a-t-il pas réalisé la plupart de ses exploits les plus valeureux sur la mer ? Ballotté sur une mer hostile, il a été jeté sur l'île d'Éole. Malgré la bienveillance des maîtres des vents, ses épreuves continuèrent. Finalement transporté par des marins phocéens, il est déposé endormi sur un rivage d'Ithaque. Ses qualités ne sont-elles pas celles qu'on exige habituellement des marins : astuce et vigueur, persuasion, ingéniosité et vaillance ? Aussi, il y a lieu de s'étonner sur le fait que le roman maritime soit resté aussi longtemps marginal dans l'histoire de la création littéraire. Que de domaines il touche pourtant : pirates et corsaires, grands capitaines ou petits mousses, explorateurs et caboteurs, pêcheurs et trafiquants, tous se croisent dans des épopées, de grandes expéditions, des aventures interlopes. Le succès éditorial, si l'on considère sa montée en puissance et l'affirmation progressive d'un genre en tant que tel, depuis le XVIII^e siècle mais essentiellement aux XIX^e et XX^e, prouve que le roman maritime rencontre un public fidèle au fil du temps, passionné et toujours demandeur, même s'il peut sembler au profane que les histoires de mer doivent toujours se ressembler un peu. On se souviendra de la critique de Théophile Gautier à son sujet, lequel considérait que le roman maritime ne faisait que broder toujours sur le même sujet. On a coutume de fixer son lieu de naissance en Grande-Bretagne. Toujours est-il qu'il émerge véritablement au cours des années 1830. Des auteurs de renom lui ont donné ses lettres de noblesse comme Eugène Sue. Fils de médecin, il débuta comme aide-chirurgien naval, et ses premières œuvres relèvent du roman naval (*La Salamandre*, 1832). Un des grands mérites d'Odile Gannier est d'en fournir une analyse complète. Elle en

démontre les ressorts en nous fournissant un savant jeu de construction navale. Tour à tour, elle fournit une typologie du roman maritime et des genres voisins. S'interroge sur la puissance narrative de ce genre, la force de sa description, la vigueur de sa prose poétique. Le roman maritime est un genre multiple ; il relève tout à la fois du roman historique, du roman éducatif, plus encore, cela va de soi, du roman d'aventure ou du roman baroque. Il scrute l'autre face de la mer, pirates et corsaires, négriers et aventuriers ; il exalte les travailleurs de la mer. Quelle multiplicité de thèmes : voyages d'exploration, voyages extraordinaires, motifs maritimes, dangers de la navigation, courses en mer, bonnes et mauvaises rencontres, combats navals bien sûr. Le roman maritime dut son succès à celui des feuilletons. Plus encore, Odile Gannier restitue le chant de l'équipage, ces innombrables formes personnelles du roman maritime. Sur ce point encore, on est frappé par la richesse de ses analyses. Elle décortique et illustre avec de nombreux extraits comment sont décrites les histoires de marins, les héros, leur langue, leurs multiples ruses et bonnes fortunes. Le modèle du récit maritime est celui du récit personnel. Il a une forme originale, celle du journal de bord, obligation professionnelle qui constitue le matériau d'écrits narratifs ultérieurs. Le journal se mue vite en fiction. Autant de journaux que de marins, de passagers et chacun se livre à des mises en forme spécifiques. Le style du roman maritime apparaît « sans apprêt », des événements remarquables aux péripéties, du rapport de mer au roman. La mythification du héros et la validation du genre, c'est au-delà du miroir de la mer, leur voix universelle, une voix unique, mer et métaphysique.

- Dressés dès la fin du XV^e siècle dans l'estuaire de la Gironde, avec le phare de Cordouan, puis à la pointe de la Bretagne, jaillis du creux des vagues, comme bâtis sur la houle : les phares. Qu'ils soient en pierre, en béton, en métal, dressés au milieu des

flots sur un frêle récif, plus souvent reposant à terre sur une pointe, un cap, l'entrée d'un port, d'un estuaire, le phare constitue un élément indissociable du paysage marin. D'où vient la fascination qu'il exerce, outre le fait qu'il s'agit à notre époque d'une aventure révolue avec l'avènement du radio guidage et du *GPS* ? Sans doute provient-elle du mystère de sa lumière qui jaillit dans la nuit noire ou du destin des hommes qui les ont marqués de leur empreinte ? Ou de ceux qui les ont conçus et de ceux qui y ont vécu en ermites : les gardiens du feu ? Dès leur construction à la fin du XIX^e siècle, les premiers phares en mer ont suscité une littérature extrêmement variée, inspirant des écrivains aux sensibilités aussi différentes que celles d'Alphonse Daudet et de Rachilde, d'Anatole Le Braz et de Jules Verne. À cette première vague littéraire succédèrent, au XX^e siècle, non seulement des romans mais aussi des récits, témoignages

ou reportages. Vincent Guigueno, ingénieur de l'École Polytechnique et de l'École des Ponts et Chaussées, docteur en histoire de l'Université Paris I, chargé de recherches, responsable du patrimoine « phares et balises » à la Direction des Affaires maritimes, commissaire de l'exposition sur les phares au musée national de la Marine restituée dans son ampleur l'histoire des phares, de leur vie, celle d'un bateau de pierre, de l'ensemble des « aides à la navigation » : tourelles, bouées, balises, amers. En 1800, la France comptait une quinzaine de phares ; soixante-dix ans plus tard on en dénombrait 291, dont celui de Ar-Men édifié à l'extrémité de la chaussée de Sein, dont la construction aura duré quatorze ans de 1867 à 1881 ! À cette date, Paris est devenu la capitale industrielle des phares, sa production illumine le monde.

Eugène Berg

MÉDITERRANÉE

Espaces maritimes et articulations transnationales : le cas de la Méditerranée

Rapport de l'atelier LittOcean ⁽¹⁾, le 12 avril 2012 à l'École militaire.

Ce premier atelier de *LittOcean* visait à comprendre les conséquences de la globalisation sur la gouvernance et la gestion de l'espace maritime dans le bassin méditerranéen et les transformations qui en résultent sur le plan des processus de décision. L'interface terre-mer, souvent restreint à des approches sectorielles compartimentées, devient de nos

jours un enjeu socio et géopolitique du développement durable.

La mer, la plus souvent perçue de la terre, prend une importance nouvelle et pose le problème de son appréhension par les acteurs sociaux et les décideurs politiques. L'action publique se trouve ainsi confrontée à de nouvelles règles du jeu, voire contrainte à imaginer et innover d'autres principes de régulation en les co-construisant avec de nouveaux acteurs situés en deçà comme au-delà des frontières nationales.

L'atelier *LittOcean* avait pour objectif, grâce à ses trois tables rondes ⁽²⁾, de créer un lieu de débat et de prospective sur ces questions, en s'appuyant sur les processus émergents (du local au global), tant dans les représentations,

(1) *LittOcean* - « Pour des espaces maritimes équitables », 36, rue de Bellechasse, 75007 Paris (www.littocean.fr). Membres fondateurs : Cécile Grignon-Logerot, Bernard Kalaora, Catherine Bersani, Christophe Pipolo, Yves Henocque, Christophe Le Visage, Anne-Sophie Leclère, Xavier Lafon.

(2) 1. Diversité des contours et des problématiques du bassin méditerranéen ; 2. Réconciliation des approches pour une cohérence des principes ; 3. Sécurité intégrale de l'espace maritime méditerranéen.

valeurs, pratiques et projets innovants concernant la gouvernance pour la sécurité d'une mer riche d'histoire, de plus en plus investie par les hommes que dans leurs *artefacts* scientifiques, techniques, d'ingénierie industrielle et écologique. Parmi les personnalités présentes ⁽³⁾, des experts en stratégie et politique maritime, dont un expert, théoricien et praticien de la stratégie et de la planification dans le domaine de la sécurité, des décideurs et gestionnaires impliqués dans l'action publique, des chercheurs issus de disciplines différentes (sciences sociales et sciences de la nature), tous issus d'institutions diverses.

2011, année de transition stratégique

La réalité de la Méditerranée reste indéterminée et imprécise. Son histoire est une histoire de passages au travers des « cinq méditerranées » que sont la Méditerranée extérieure (Mauritanie, Maroc, Portugal), la Méditerranée occidentale (Europe du Sud et Afrique du Nord), la Méditerranée orientale (Balkans, Albanie, Grèce, Turquie, Chypre et Égypte), la Méditerranée arabe (Proche-Orient, mer Rouge, golfe Persique) et la Méditerranée caucasienne (zone de la mer Noire). L'histoire de ces différentes méditerranées a laissé de profondes cicatrices avec des représentations, de l'intérieur et de l'extérieur, qui ne convergent pas. Dans ces conditions, comment peut-on parler de vision collective alors que les problèmes sont loin d'être réglés dans un processus de Barcelone qui s'est peu à peu enlisé ? Une nouveauté cependant, que l'on a appelée le « Printemps arabe », véritable révolution des sociétés arabo-musulmanes autour d'un rééquilibrage de leurs trois pôles que

sont le politique, le social et le religieux, dans une situation figée où le politique s'était petit à petit complètement détaché du social alors que le religieux, lui, avait comblé le vide en investissant largement le pôle social.

Parmi les « dopants » régionaux de cette transition stratégique figurent la confusion qu'a entraînée l'intervention en Irak, la publication des analyses *Wikileaks* sur les échanges avec les pouvoirs en place, et une prise en compte collective de la réalité, particulièrement portée par le média régional et mondial qu'est la chaîne *Al Jizera*.

À des stades différents selon les pays, la révolution arabo-musulmane ouvre indéniablement la voie à un processus démocratique avec, a) en termes d'enjeux, la capacité à trouver un nouveau point d'équilibre, l'évolution des relations entre le bloc arabo-méditerranéen et le bloc euro-méditerranéen ; b) en termes de risques, l'impatience des peuples autour du triptyque indissociable dignité-liberté-prospérité, la confusion entre crise systémique et crise arabo-musulmane, la mondialisation de la démocratisation ; et c) en termes d'atouts, la libération de la parole et de l'énergie, le dialogue des générations vers une vision trans-générationnelle, la fin des tabous et des dogmes, et de manière générale un contexte économique relativement plus favorable lié aux performances du continent africain.

Un espace maritime méconnu

Étymologiquement, le sens latin de « Méditerranée » est celui de la « mer au milieu des terres », alors que, malgré les écrits de visionnaires comme Fernand Braudel, la vision d'aujourd'hui reste plutôt celle des « terres qui entourent la mer », que ce soit sur les plans géographique ou géopolitique.

Au long de l'histoire, la Méditerranée apparaît comme une zone de contact à la jonction des trois continents que sont l'europpéen, l'africain et l'asiatique, avec ses éléments de

(3) Tous les intervenants sont membres de *LittOcean* : amiral Jean Dufourcq, École militaire, Membre d'honneur *LittOcean* ; Bernard Kalaora, EHESS, Président de *LittOcean* ; Catherine Bersani, Inspecteur général de l'Équipement ; Christophe Le Visage, Stratégies Mer et Littoral ; Yves Henocque, Ifremer ; Anne-Sophie Leclère, Agence de l'Eau ; Julien Rochette, IDDRI ; Julia Jordan, UPM.

convergence, moteurs de la coopération bilatérale et multilatérale mais également ses éléments de divergence qui mènent aux conflits. On a donc affaire à une mer fermée certes mais un espace ouvert au monde qui crée du lien entre les différentes régions qui la bordent. La zone d'intersection commune entre ces régions, la zone d'interface, c'est bien la mer, une mer dont 70 % des eaux sont classées « eaux internationales » selon la Convention des Nations unies sur le droit de la mer, interdisant ainsi toute intervention significative sur cet espace partagé mais également « ignoré » par tous. Ainsi, face à une Méditerranée plurielle, comment faire en sorte que cet espace maritime devienne une zone d'interface positive, à quel dispositif pluriel mais cohérent de gouvernance faudrait-il parvenir pour donner des objectifs communs aux régions qui l'entourent ?

À propos de la vision Nord-Sud

L'Union européenne est devenue le premier partenaire économique d'Israël et le premier contributeur de l'aide internationale apportée aux territoires palestiniens. Cependant, en dépit d'une position commune affirmée à Venise en juin 1980 et de la mise en place du processus euro-méditerranéen à Barcelone en 1995, dans la foulée des accords d'Oslo qui marquaient un premier jalon vers la paix, l'UE n'est toujours pas considérée comme un véritable interlocuteur politique dans la région. Sans geste politique fort en direction des ennemis héréditaires que sont Israël et la Palestine, l'Union pour la Méditerranée (UPM), voulue par la France et arrimée à l'Union européenne par la volonté de l'Allemagne, risque d'achopper sur les mêmes difficultés que le processus euro-méditerranéen. Les projets concrets que l'UPM cherche à promouvoir dans le domaine de l'eau, de la recherche agronomique, de la protection civile, sont certes utiles mais la recherche de la paix dans cette région proche, qui demeure la zone de conflits et de tensions

la plus dangereuse du monde et où le temps ne joue pas en faveur des modérés, devrait être une priorité politique.

Pour une sécurité durable

Parler de paix c'est, au-delà du simple aspect militaire, parler des conditions d'une sécurité durable : sécurité humaine bien sûr (besoins vitaux de l'homme) et sécurité culturelle alors que les conditions favorables sont encore loin d'être réunies dans bien des pays et bien des régions. Les cas de litige historique, nombreux, ne pourront être soldés que si finalement ce sont les Méditerranéens eux-mêmes qui prennent la main. À ce titre, des lieux de dialogue et d'action comme le 5+5 (Méditerranée occidentale) mériteraient d'être dupliqués vers d'autres « méditerranées » (orientale, arabique, caucasienne) afin d'expérimenter des méthodes qui pourraient s'appliquer par exemple à la circulation humaine⁽⁴⁾.

La construction d'une gouvernance maritime de la Méditerranée dépendra de cette capacité de dialogues et de la création des conditions nécessaires à une sécurité durable.

Mais dire cela nous amène à reconnaître qu'en dépit de nos meilleures intentions la complexité systémique et culturelle du monde présent rend souvent nos décisions contraires aux résultats que nous voulions atteindre. Ce dont nous avons le plus besoin aujourd'hui, c'est de réviser nos modèles d'intervention qui sont à la source de bon nombre d'incompréhensions, plutôt que de

(3) « De longue date, les migrations de l'Afrique subsaharienne vers l'Afrique du Nord peuvent être valablement comparées à celles du Maghreb vers l'Europe, que ce soit par les dimensions politique et culturelle ou par le rôle des *diasporas* dans l'aide aux régions d'origine. Qu'il s'agisse de franchir le Sahara ou la Méditerranée, les caractéristiques des réseaux clandestins ne sont pas fondamentalement différentes et la problématique des zones de rétention est la même, que ce soit au Maghreb ou en Europe ». Cf. « L'intégration de l'espace méditerranéen et de l'espace euro-africain », Forum Mondial du Développement Durable, juillet 2001.

vouloir planifier l'avenir ou mener à terme un projet prétendant structurer le monde à venir. Le monde présent demande d'être ouvert et à l'écoute non pour réguler l'imprévisible mais pour être plus attentif à l'environnement qui nous entoure et trouver les réponses appropriées à un monde dont les imbrications provoquent des ruptures et changements que nous ne pouvons plus prévoir.

Dans les réseaux de recherche et d'expertise pour des espaces maritimes équitables, auxquels *LittOcean* ambitionne de contribuer, la question est bien celle de penser autrement les stratégies d'intervention que le font les organismes européens ou internationaux en Méditerranée et dans le reste du monde.

Yves Henocque
Ifremer

RUSSIE

La longue route de la Russie vers l'OMC

Le 16 décembre 2011, l'Organisation mondiale du commerce (OMC) accueillait officiellement la Russie dans ses instances genevoises. La signature, le mois précédent, d'un accord bilatéral entre la Russie et la Géorgie avait levé le dernier obstacle sur la route de Moscou à Genève et la *Douma* dispose maintenant jusqu'à juin 2012 pour ratifier une adhésion historique.

Après 18 années de négociation (battant au passage le record de 14 ans précédemment détenu par la Chine), le pays deviendra dès lors le 154^e État-membre de l'Organisation présidée par Pascal Lamy. Lequel déclarait d'ailleurs le jour de la signature de l'accord que « jusqu'à l'adhésion de cet important pays, nous ne pouvions pas véritablement être l'Organisation "mondiale" du commerce ». Après l'échec du cycle de négociations de Doha, cet élargissement vers l'Est apporte en effet un nouveau souffle à l'OMC qui couvre désormais 97 % du commerce mondial. Surtout, il met fin à l'isolement de la Russie, dernière grande économie absente de l'OMC, rompant avec l'idée d'un certain particularisme intrinsèquement russe, que chantait déjà le poète Fiodor Tioutchev au XIX^e siècle : « On ne

peut pas comprendre la Russie par la voie de la raison / On ne peut pas la mesurer / Elle a un caractère particulier / On ne peut que croire en elle ». La Russie, neuvième économie mondiale et premier exportateur d'énergie, est désormais officiellement intégrée à la mondialisation.

Toutefois, comme le souligne Elvira Nabiullina, ministre du Développement économique de la Fédération de Russie, « rejoindre l'OMC n'est pas une fin en soi mais un début ». Les économistes de la Banque mondiale, Thomas Rutherford et David Tarr, estiment que l'entrée de la Russie dans l'OMC apportera au pays 3,7 % de croissance du PIB supplémentaire lors des cinq prochaines années et 11 % à long terme. Alexeï Koudrine, l'ancien ministre des Finances démissionnaire en septembre passé, considère pour sa part que l'adhésion fournira entre 3 et 4 % de croissance additionnelle au pays lors des dix prochaines années. D'après l'étude de la Banque mondiale, les bénéfices de cette adhésion pour l'économie nationale pourraient être classés en trois catégories : a) 72 % des gains seraient liés à l'amélioration de la qualité et à la baisse des prix des services, qui devraient contribuer à accroître la profitabilité et la compétitivité des sociétés russes ; b) 18 % à la réduction du prix des biens grâce à la baisse des tarifs douaniers ; c) 10 % au meilleur accès des sociétés exportatrices russes aux marchés étrangers (notamment

de métaux et d'engrais, les deux secteurs représentant ensemble 20 % des exportations du pays, tandis que les barrières douanières sur l'énergie sont déjà peu élevées). En effet, l'OMC offre désormais à l'État russe un arsenal juridique pour défendre les droits et intérêts de ses entreprises si des États venaient à dresser inopinément de nouvelles barrières commerciales. Pour maximiser ces bénéfices, la Russie devra aussi améliorer son climat des affaires, le pays étant aujourd'hui classé 120^e sur 183 dans l'indice « *Doing business* » de la Banque mondiale. De ce point de vue, l'OMC offre à Moscou l'occasion de mettre en place un environnement commercial et juridique plus prévisible et transparent, indispensable pour attirer davantage d'investissements directs étrangers (IDE).

Bien entendu, l'adhésion de la Russie suscite aussi des craintes. D'une part du fait de l'importance historique des douanes russes dans la vie économique et politique du pays car réduire les tarifs douaniers revient par la même occasion à diminuer les entrées d'argent pour l'État. D'autre part parce que la réduction de ces barrières douanières exposera les entreprises russes à davantage de concurrence étrangère. Aleksandr Shokhin, à la tête de l'Union russe des industriels et entrepreneurs, considère ainsi que les secteurs jugés vulnérables (production et équipement agricole notamment) nécessiteront plus de 13 milliards de dollars d'aides publiques pour affronter leurs homologues étrangers. Mais le traité d'adhésion signé à Genève autorise le gouvernement russe à accorder 9 milliards d'aides au secteur agricole en 2012 et 2013 (soit près du double des sommes engagées par l'État en 2011) lesquelles seront amenées à diminuer progressivement.

Dès lors, pourquoi avoir attendu dix-huit ans avant de rejoindre l'OMC ? Et pourquoi sauter le pas en 2012 ?

Premier élément de réponse, l'économie russe est plus mature et compétitive aujourd'hui qu'au début des années 90. N'oublions

pas que ce n'est qu'en 2007 que le PIB russe a dépassé en termes réels le niveau qui était le sien en 1989. Deuxièmement, la question des tarifs douaniers est devenue moins sensible depuis que les exportations énergétiques les ont remplacés comme première source de revenus de l'État. Des exportations de pétrole qui apportent plus de 900 millions de dollars au pays chaque jour au prix actuel du baril de brut. Enfin, ce mariage tant attendu doit aussi être replacé dans le contexte de la crise économique mondiale actuelle qui a fait prendre conscience au pouvoir russe de la fragilité de son modèle économique. Après une contraction de 7,9 % en 2009, le PIB a crû de 4,4 % en 2010 et de 4,3 % en 2011. Un niveau enviable pour bien des économies occidentales mais largement en dessous du niveau de leurs homologues émergents et de moitié inférieur à la croissance du pays avant la crise. Certes, l'économie russe dispose d'atouts certains et a fait preuve d'une impressionnante vigueur depuis la crise financière de 1998. Le PIB a crû de près de 7 % par an de 2000 à 2008, le pays dispose aujourd'hui des 3^e réserves mondiales (520 milliards de dollars) après la Chine et le Japon et devant l'Arabie saoudite, et la dette publique ne représente que 10 % du PIB, contre 66 % en 1997.

Cependant, malgré ces réussites, le modèle reste vulnérable. D'abord du fait de son extrême dépendance aux cours des matières premières. Les hydrocarbures représentent 65 % des exportations du pays, et pour atteindre l'équilibre, le budget 2012 nécessite un baril de pétrole à 115 dollars, contre 30 en 2007. Une tendance qui risque fort de s'accélérer au vu de la probable augmentation des dépenses publiques suite aux promesses de la campagne électorale. Seconde source de fragilité, le faible niveau d'investissements, lesquels représentent aujourd'hui 22 % du PIB contre 26 % en 2008, insuffisant pour renouveler le gigantesque appareil productif du pays. Pour la seule organisation de la Coupe du monde de

football 2018, le pays devra ainsi investir plus de 50 milliards de dollars en infrastructures, soit 3 % du PIB national. Un défi brutalement porté sur le devant de la scène après l'accident de la centrale hydro-électrique de Sayano-Shushenskaya (6^e au monde par sa taille) en août 2009 et lié à une autre menace : la fuite des capitaux. D'après les données de la Banque centrale, 84 milliards de dollars ont quitté le pays en 2011 ; le double de 2010. Une fuite toutefois largement équilibrée par le solde positif de la balance des paiements, du fait des exportations d'hydrocarbures.

Comment dès lors tirer parti de l'immense potentiel économique du pays ? En diversifiant l'économie et en attirant davantage d'IDE. De ce point de vue, l'adhésion à l'OMC s'inscrit dans la continuité du discours modernisateur « des 4 I » prononcé par Dimitri Medvedev en février 2008 à Krasnoïarsk : Institutions, Infrastructures, Innovation, Investissement.

Bien entendu, l'OMC offre une large marge de manœuvre à ses États-membres, qui sont loin d'avoir tous laissé grandes ouvertes leurs frontières. Les effets positifs de l'adhésion ne

se feront peut-être sentir qu'à long terme et nécessiteront sans doute une première période d'ajustements parfois douloureux. Néanmoins, il est permis d'imaginer que cette décision, même symbolique, marque un certain tournant et le début d'une nouvelle ère dans l'histoire postsoviétique du pays.

Les années 90 furent la décennie de la transition économique et de la transformation politique. La décennie 2000 fut, quant à elle, marquée par la croissance économique et le renforcement de l'État, deux phénomènes appuyés par le développement du secteur énergétique. Les années 2010 seront-elles celles de la diversification économique et de la construction d'un État de droit ? Le défi est immense mais répond aux attentes d'une classe moyenne qui représente aujourd'hui 25 % de la population, contre 5 % seulement dans les années 90, et qui compte désormais faire entendre sa voix.

Avril 2012

Alexandre Kaufmann

NDLR - Les vues exprimées dans cet article sont personnelles et n'engagent pas la Banque européenne pour la reconstruction et le développement où travaille l'auteur.

ASIE

Trois théâtres « chauds »

Le théâtre afghano-pakistanaï et ses approches

En dehors du site ⁽¹⁾ de la Force internationale d'assistance et de sécurité (Fias) ⁽²⁾, très peu d'informations émanent sur les opérations conduites par l'Otan en Afghanistan contre les *taliban* dont la vigueur activiste demeure forte. Elle se manifeste en particulier par la perpétration d'attentats ou d'attaques contre des objectifs significatifs

tels que parfois le cœur d'installations de l'Otan. En outre, plusieurs maladroites américaines individuelles graves telles que le malencontreux autodafé de corans à la mi-février ou le massacre de seize Afghans le 11 mars à Kandahar, viennent compliquer la conduite globale des opérations. Ces événements sont d'une gravité telle qu'ils contraignent les très hauts responsables américains à intervenir directement auprès du gouvernement Karzai pour tenter un replâtrage d'une confiance partenariale de plus en plus ébranlée.

C'est dans cette ambiance tendue que se prépare l'extraction anticipée des forces de l'Otan, sur le terrain des combats cependant et non pas ceux du soutien ni de la formation.

(1) Cf. (www.isaf.nato.int/article/news/index.php).

(2) Ou *International Security Assistance Force (ISAF)*.

Résultat de l'insistance du gouvernement afghan autant que de la volonté politique de plusieurs des pays engagés dans ce théâtre, ce désengagement devrait être achevé vers la mi-2013, soit un an plus tôt que prévu, à la faveur d'un transfert accéléré des responsabilités aux forces nationales afghanes de défense et de sécurité (FNADS). Les autorités politiques alliées, réunies dans le cadre des consultations régulières globales au niveau des ministres de la Défense et des Affaires étrangères les 18 et 19 avril à Bruxelles, insistent sur le fait qu'il n'y a pas contradiction en cela avec le programme dit de Lisbonne, arrêté le 20 novembre 2010, programme qui, entre autres, prévoit que les transferts soient effectivement achevés en 2014. Ceux-ci se poursuivent effectivement sur le terrain. Ainsi le 3 avril, les Britanniques en ont réalisé un sur la dernière tranche du secteur de Lashkar Gah, dans la province d'Helmand. Le 8 avril, un accord opérationnel a été établi entre Américains et Afghans attribuant désormais la responsabilité des opérations de nuit aux Afghans. Enfin les effectifs des FNADS s'étoffent. Aujourd'hui composés de 344 108 militaires et policiers, ils devraient atteindre en octobre l'objectif fixé de 352 000 individus.

Après 2014, l'Afghanistan ne sera pas pour autant abandonné puisque la réunion de Bruxelles a été aussi l'occasion d'élaborer un plan de soutien aux FNADS, soutien dont le budget est pour l'heure calculé à hauteur de quelque 4 milliards de dollars. Ce plan est en outre complété par un accord de partenariat stratégique que, à l'occasion d'un voyage surprise qui coïncide avec la date anniversaire de l'élimination de Ben Laden, le président Obama en personne vient de signer avec son homologue afghan à Kaboul, le 1^{er} mai.

Les opérations de lutte contre les résidus d'*Al-Qaïda* et les *taliban* se heurtent aussi aux graves problèmes relationnels entre les États-Unis et un Pakistan qui n'a toujours pas admis que l'opération de destruction de Ben Laden par les forces américaines le

1^{er} mai 2011 ait pu être conduite sur leur territoire sans leur consentement préalable, un Pakistan qui refuse de croire à une erreur de trajectoire de missile américain contre l'un de ses poste-frontières le 26 novembre 2011, un Pakistan qui du coup a interdit que son territoire demeure « ligne de communications » du soutien logistique des forces alliées en Afghanistan et qui veut imposer des conditions drastiques à la réouverture de cette dernière. À noter que, face à cette situation les Russes, qui voient avec une inquiétude grandissante l'échéance du retrait de l'Otan, ont, pour compenser, offert de mettre la base d'Ulyanovsk⁽³⁾ à la disposition des alliés pour assurer une partie de leur logistique par voie aérienne.

Quant aux opérations que les Pakistanais sont censés mener dans le Nord Waziristan, elles paraissent engagées sans grande conviction. Imposées par les attaques d'insurgés ou de *taliban*, elles ne semblent être de ce fait que des réactions de circonstance plutôt que des actions volontairement décidées. Alors que sur l'ensemble du théâtre les résultats apparaissent loin d'être décisifs et la stabilité régionale loin d'être assurée, l'on s'achemine néanmoins vers des négociations de retour au calme plutôt que d'authentique retour à la paix. À cette fin, Afghanistan, Pakistan et Iran se concertent le 16 février, tandis que, de leur côté, les États-Unis engagent au Qatar des pourparlers préliminaires avec les *taliban* qui dédaignent les appels du président Karzai à engager des discussions directes avec son gouvernement.

Sur le plan stratégique, le Pakistan, se sentant à tort ou à raison pris en tenaille entre l'Afghanistan et l'Inde, effectue une nouvelle approche en direction de l'Inde qui, pour l'heure, la reçoit favorablement mais avec quelques réserves cependant. Le 29 février, Islamabad annonce qu'il normalisera ses relations commerciales avec New Delhi

(3) Chef-lieu de l'oblast du même nom ; située sur la Volga à 893 kilomètres de Moscou.

avant décembre. Le 8 avril, Asif Ali Zardari, accomplit la première visite présidentielle pakistanaise en Inde depuis 2005. Une volonté commune de reprendre des relations de bonne qualité est affichée. Des mesures concrètes sont décidées. Mais l'Inde demande toujours des comptes sur l'opération terroriste perpétrée en 2008, à Mumbai, par le groupe *Lashkar-e-Taiba*, dont le *leader* Hafiz Mohammad Saeed réside librement au Pakistan.

Il n'empêche que, dans le cadre de la consolidation de leurs défenses respectives, les deux États procèdent à des essais de missiles à capacité soit conventionnelle, soit nucléaire. De son côté, Islamabad en a réalisé deux : un le 5 mars d'un missile *Hafiz-2*, à courte portée, et le 25 avril d'un *Shahen I* modernisé, à moyenne portée. Quant à l'Inde, c'est le lancement d'un *Agni-V*, missile nucléaire à longue portée, qu'elle réussit le 19 avril. Cela dit, ce succès indien ne peut occulter l'état de décrépitude que connaît l'armée régulière, décrépitude portée à la connaissance du grand public à la suite de fuites émanant du ministère de la Défense.

Sur le plan de la politique internationale, le 29 mars a consacré un moment important pour l'Inde puisqu'elle a accueilli le quatrième Sommet des Brics (Brésil, Russie, Inde, Chine, Afrique du Sud), Sommet au cours duquel il est décidé de créer une nouvelle banque de développement par les Brics et pour les Brics. L'objectif est de fournir aux pays concernés un système bancaire commun qui leur éviterait de subir les contre-coups des crises monétaires occidentales. Le Sommet a été aussi l'occasion de prendre une position commune en faveur du droit de l'Iran à une utilisation pacifique de l'énergie nucléaire et de lancer un avertissement sur les « conséquences désastreuses » qui s'ensuivraient si la contestation sur le programme nucléaire militaire iranien devait s'orienter vers une solution de violence. L'Inde est d'autant plus soucieuse des

sanctions appliquées à l'Iran qu'elle en dépend fortement pour ses approvisionnements en pétrole. Quant au problème syrien, tous ont reconnu qu'il devait se traiter en interne et dans le respect de l'indépendance et de la souveraineté du pays.

Le théâtre Sud-Est asiatique autour de la mer de Chine du Sud

Si les tensions ne s'apaisent pas en Asie du Sud parce que, pour l'heure, elles restent essentiellement liées à la persistance de la crise afghane en mauvaise voie de résolution, d'autres tensions se créent en Asie du Sud-Est. Elles se cristallisent autour de la mer de Chine du Sud sur laquelle Pékin marque de plus en plus résolument sa volonté d'en faire une mer strictement chinoise. À cette volonté s'opposent surtout celles du Vietnam et des Philippines qui entendent préserver ce qu'ils estiment y être leurs droits souverains face aux prétentions abusives chinoises, prétentions selon lesquelles Pékin, rappelons-le, entend s'arroger la quasi-totalité du bassin par le biais d'un « tracé en neuf traits », héritage d'un dessin non officiel remontant à 1947. Dans les faits, cela se traduit par des arraisonnements arbitraires de bateaux de pêche vietnamiens, accusés d'avoir pénétré indûment dans les eaux territoriales chinoises des îles Paracels, îles dont les Chinois ont achevé de s'emparer par la force en 1974 et sur lesquelles la souveraineté chinoise n'est pas juridiquement avérée.

Pour l'heure, les confrontations les plus graves se produisent avec les Philippines qui, assurées d'un discret soutien américain, refusent résolument de se laisser impressionner malgré la pauvreté de leurs moyens militaires. Les pressions chinoises sont multiples et rudes. Elles se manifestent dès le 29 février lorsque les Philippines font part de leur intention d'ouvrir à la coopération internationale, à partir du mois d'avril, deux blocks pétroliers dans le secteur de *Reed bank*, hauts fonds non découvrants du plateau continental

philippin, situés au nord des îles Spratleys. Elles se manifestent encore lorsque les Philippines annoncent leur projet de moderniser leurs installations sur l'île de Paga-asa, île que ceux-ci occupent dans ce même archipel. Et aussi lorsque Vietnamiens et Philippines entreprennent de réaliser un exercice naval commun également dans les Spratleys. Enfin, tout au long des trois dernières semaines d'avril, les Chinois entendent défendre par la force les droits non fondés de leurs pêcheurs à exercer leurs activités dans l'atoll effondré de Scarborough Reef, à quelque 230 km de la côte la plus proche des Philippines et sur lequel les Chinois prétendent à souveraineté. Cette dernière confrontation, qui en reste cependant au niveau des expressions mutuelles de défiance, fait ressortir davantage, chez les Philippines, le besoin de renforcer leurs moyens navals, ce que le 22 avril le commandant des forces de sécurité exprime ouvertement.

Quant au soutien américain, sans que ce soit pour l'heure un appui, il est désormais acquis, que ce soit au travers de la promesse de fournir des équipements militaires, notamment navals, et du renforcement des entraînements militaires communs. Ce qui est le cas lors de l'exercice annuel *Balikatan* (Épaule contre épaule), exercice antiterroriste qui, contrairement aux autres années où il avait lieu sur l'île de Mindanao, se déroule en 2012, du 16 au 27 avril, dans la province de Palawan, qui a juridiction sur la partie philippine des îles Spratleys. Il n'en faut pas plus pour faire réagir violemment la Chine qui considère l'exercice comme une menace pour la stabilité régionale.

Le problème qui continue à se poser pour les pays de l'ASEAN à propos de la mer de Chine du Sud est leur manque de solidarité sur laquelle joue la Chine. Cela a été manifeste cette année à l'occasion du Sommet de l'ASEAN (3-4 avril) dont la présidence revient au Cambodge. Pour ne pas déplaire à la Chine et considérant que la question de

la mer de Chine du Sud n'est pas un problème entre la Chine et l'ASEAN mais entre la Chine et les parties prenantes, ce qui est exactement la position chinoise, Phnom Penh a refusé d'inscrire la question de la mer de Chine du Sud à l'ordre du jour du Sommet. Il y aura lieu de porter attention sur ce que sera, en 2014, l'attitude d'une Birmanie qui s'achemine progressivement vers la démocratie et qui, cette année-là, est appelée à assumer cette même présidence.

En tout état de cause l'agressivité de Pékin autour de la mer de Chine du Sud et sa volonté d'en faire une stricte mer chinoise inquiètent fortement les pays d'Asie du Sud-Est qui ont, depuis deux ans déjà au moins, entrepris d'authentiques programmes d'accroissement de leurs moyens militaires et de modernisation de leurs existants. La même inquiétude touche les États-Unis qui, avec des perspectives de budget militaire en réduction, doivent cependant trouver des palliatifs pour continuer à assurer une présence forte dans la région, à la fois pour y contrer les ambitions chinoises et y préserver, ce qui est essentiel pour eux, la liberté de la navigation. C'est pourquoi Washington resserre de plus en plus ses liens avec les pays d'Asie du Sud-Est, notamment sur le plan de la coopération militaire. L'objectif est de renforcer les capacités opérationnelles navales de ces pays pour leur permettre d'assumer une sécurité régionale plus vigoureuse qu'actuellement et suppléer ainsi à la diminution des moyens qu'y engageaient les États-Unis jusqu'à présent.

Le théâtre Nord-Est asiatique

Enfin, le troisième centre d'instabilité en Extrême-Orient se situe en Asie du Nord-Est. S'y manifeste une fois de plus la versatilité de la Corée du Nord, son nouveau *leader* Kim Jong-un semblant vouloir suivre la trace de son père. Ainsi, en début de période, Pyongyang se dit prêt à reprendre les négociations à Six sur son programme nucléaire et à accepter les visites de l'Agence

internationale à l'énergie atomique (AIEA). Mais à la fin, malgré une opposition quasi-unanime de la communauté internationale qui, pour une fois, compte la voix de la Chine, la Corée du Nord lance le 12 avril une fusée *Unha-3*, prétendument pour mettre en orbite un satellite de météorologie. Tous les spécialistes des stratégies de ce pays dénoncent l'acte comme un faux-fuyant qui camoufle la réalité d'un essai de futur missile balistique. Hélas pour les Nord-coréens, la fusée explose une minute après son décollage et ses débris se dispersent en mer Jaune. Par réaction à cet acte, pour marquer de façon concrète la désapprobation internationale, le conseil de sécurité de l'ONU décide le 2 mai d'appliquer des sanctions à l'encontre de trois entreprises nord-coréennes impliquées dans les programmes illicites nucléaires et de missiles de leur pays. Ces sanctions se traduiront par le gel à l'étranger des capitaux des dites compagnies.

En revanche, après l'insuccès du lancement de l'*Unha-3*, les mêmes observateurs opèrent un rapprochement immédiat avec l'attitude que Pyongyang avait marquée après les faillites des lancements tentés en octobre 2006 et en mai 2009. En effet, peu de temps après ces échecs, les premier et deuxième essais nucléaires leur avaient succédé. Or, depuis le 8 avril, des images satellitaires du site de Punggye-ri y révèlent d'importantes activités de préparation à un semblable essai. Ainsi alertés, les États-Unis mettent en garde la Corée du Nord contre la mise à exécution d'une nouvelle expérimentation. La Chine elle-même avertit Pyongyang, le 26 avril, que s'il persiste dans son projet, elle ne pourrait plus le couvrir.

De telles condamnations n'ont cependant pas pu être concertées à l'occasion du deuxième Sommet sur la sécurité nucléaire organisé à Séoul les 26 et 27 mars puisque, à cette époque, les projets nord-coréens sur Punggye-ri n'étaient pas encore révélés. Malgré le symbole qu'il pouvait contenir en

la circonstance, ce Sommet, qui réunissait 53 États, ne visait pas spécifiquement la position nord-coréenne en matière de menace nucléaire. Elle concourait d'abord à la recherche de solutions efficaces de prévention destinées à interdire à des terroristes l'accès aux ressources nucléaires encore dispersées dans le monde.

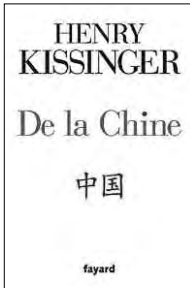
Au lancement échoué de la fusée *Unha-3*, à la préparation d'un nouvel essai nucléaire, la Corée du Nord ajoute le 23 avril la menace brutale de réduire en cendres son voisin du Sud. Ce qui suscite immédiatement les craintes de Séoul malgré les assertions renouvelées américaines de soutien alors que parallèlement, au Japon, sur la base d'un accord signé le 26 avril, se met en place un projet de dégagement vers Guam de 9 000 *Marines* jusque-là implantés à Okinawa. En contrepoint, et par ailleurs, il y a lieu de s'interroger sur la signification de la participation de la Russie à un exercice naval conduit en commun avec la Chine du 22 au 27 avril en mer Jaune : exercice dans le cadre de l'Organisation de coopération de Shanghai. Signification d'une opposition russe à un appui américain trop marqué à l'égard de la Corée du Sud alors qu'en mer de Chine du Sud, ces mêmes Russes ne marquent pas d'hostilité envers les Américains ? Souci constant de maintenir un équilibre entre Chine et États-Unis ? L'interrogation reste entière.

*
**

Au total, trois théâtres sur lesquels pèsent de sérieuses incertitudes : il y a doute sur le succès des opérations d'éradication des *taliban* en Asie du Sud ; il y a doutes sur la capacité de la communauté internationale à faire lâcher prise à la Chine dans sa volonté de s'emparer de la mer de Chine méridionale et sur la capacité de cette même communauté de réussir à ramener la Corée du Nord à la raison.

13 février – 3 mai 2012

Général (2S) Daniel Schaeffer



| Henry Kissinger : **De la Chine** ; Fayard, 2012 ; 576 pages.

C'est un grand livre que vient de publier Henry Kissinger sous le titre *De la Chine (On China)*. L'analyste subtil de la gouvernance du monde y exprime son *credo*. Sans ordre mondial sous un système de relations cohérentes plus ou moins organisées, les affrontements risquent de dégénérer en conflits dévastateurs. Depuis la Seconde Guerre mondiale, les États-Unis ont assumé la charge de la direction du système du monde par le *leadership*. Le message de Kissinger est simple : pas d'ordre mondial sans la Chine.

De quel ordre mondial s'agit-il ? Quels sont ses fondements ? Henri Kissinger a, depuis longtemps, exprimé son scepticisme sur les principes de raison d'État, de l'équilibre des forces, de *realpolitik*. La multiplication du nombre des États et leurs disparités, liées à la mondialisation, a affaibli et souvent rendu caducs ces fondements. La raison d'État ne peut correspondre aux aspirations des États-Unis et de leurs présidents, Wilson, Roosevelt ou ceux de la période de la guerre froide. Car la diplomatie de notre époque exige d'abord une coordination qui ne peut naître sans un minimum de compréhension. Là est la mission et le rôle essentiel de la diplomatie : tenir compte des potentialités, de l'instant opportun, rechercher ce qui est compatible sans sous-estimer ce qui ne l'est pas, deviner les impasses dans la recherche du moment favorable, avoir une juste appréciation des opportunités idéologiques, de façon à ne pas méconnaître les événements de politique intérieure souvent déterminants, surtout prendre la mesure de la personnalité et des aspirations des principaux responsables, comprendre leurs mobiles et deviner leur sensibilité aux contraintes des pays dont ils assument le destin et, dans cette complexité, user de patience et de sérénité pour transformer un affrontement généralisé en quasi-alliance.

C'est la tâche qu'Henry Kissinger assure avoir menée à bien et il en fait l'histoire détaillée avec une abondance d'analyses. Elles culminent dans la visite d'État de Nixon en Chine qui a entraîné une évolution majeure des relations internationales.

Au départ, tout oppose la Chine de Mao Zedong – qui a conclu, en 1950, un traité d'alliance (que Mao estime chèrement payer) avec l'Union soviétique de Staline – aux États-Unis défenseurs de Chang Kai-shek et de Taiwan. Bientôt surgit la guerre de Corée, déclenchée par Kim Il-sung et, par enchaînement, l'intervention de la Chine, sur un fond de menaces nucléaires qui laissent Mao impavide. Les États-Unis et la Chine sont en guerre ; en Corée mais aussi à Taiwan où les Chinois bombardent les îles Quemoy et Matsu, avec subtilité toutefois, seulement les jours impairs et pas les jours fériés. Après la mort de Staline, Khrouchtchev s'impose, critique Staline. L'idéologie qui avait rapproché Pékin et Moscou les sépare. Khrouchtchev proclame la coexistence pacifique. Mao assure ne pas craindre la guerre. En fait, c'est l'URSS qui se lance dans l'aventure : à Cuba, en Angola. Mao, sur la réserve, affirmera que l'URSS voit dans la Chine une deuxième Yougoslavie. La seconde crise de Taiwan éclate néanmoins, en 1958, et Foster Dulles mène sa « coexistence combative ». Suit une décennie de crises

marquées par les événements intérieurs en Chine (le « grand bond en avant », la révolution culturelle) et la guerre sino-indienne de 1962.

C'est alors que Nixon et son conseiller Kissinger entrent en scène. Tout change, lentement. Mao ressort de leur exil les quatre maréchaux (Chen Yi, Nie Rongzhen, Xu Xingquian, Ye Jianying) pour une appréciation de la situation et donc des possibilités de contacts avec les États-Unis, selon la stratégie traditionnelle : s'allier au barbare le plus éloigné contre le barbare le plus proche. Viennent alors les heurts sino-soviétiques sur l'Oussouri, où les Soviétiques concentrent un million d'hommes. La « révolution dans la politique étrangère » est en marche. En 1971, Kissinger rencontre Zhou Enlai à Pékin, en mission secrète ; en février 1972, Nixon effectue sa visite en Chine. Les discussions s'engagent avec Mao et Zhou Enlai. Les difficultés sont immenses. Mais Kissinger veille à les surmonter, aidé par Zhou Enlai. Taiwan, difficulté permanente, fait l'objet d'un arrangement scellé dans un communiqué ; l'hégémonie est bannie et cette condamnation vise l'Union soviétique. Désormais, États-Unis et Chine sont dans une quasi-alliance qui « a ceci de particulier que les partenaires s'appliquent à coordonner leur action sans définir d'obligation formelle à le faire ». L'exemple vietnamien en est l'illustration : la Chine assure qu'elle ne combattrait les Américains qu'en Chine, pas au Vietnam. Pour Mao, il s'agit d'endiguer « la puissance soviétique selon une ligne horizontale » (des États-Unis au Pakistan, à l'Iran jusqu'à l'Europe), vision que Mao abandonne bientôt au profit d'une théorie des trois mondes qui laisse à la Chine une plus grande liberté d'action. Par ces ajustements, une concertation stratégique nouvelle est née. Elle bouleverse le système du monde.

Mais « tout change », comme aime à le souligner la pensée chinoise. Comment « comprendre ce qui est mouvant » se demande Henry Kissinger. Aux États-Unis, le *Watergate* emporte Nixon. En Chine, Zhou Enlai puis Mao meurent. Ressurgit alors « l'indestructible Deng ». Les portraits sont les aspects les plus passionnants de l'ouvrage. À côté de Mao « d'une autorité et d'une influence écrasantes, impitoyable et distant, poète et guerrier, prophète et fléau, qui a unifié la Chine et l'a engagée dans un voyage qui a failli détruire la société civile », il y a Zhou Enlai, figure élégante à la pensée subtile, qui rend lumineuses les assertions brutales de Mao. Puis vient Deng Xiaoping, le prophète du « réformer et s'ouvrir », apparence frêle mais d'une volonté sans mesure, réaliste et souple dans ses appréciations, implacable lorsque la situation l'exige. Il le montrera sur la place Tian an men, lorsque l'ordre sera menacé. Il n'hésitera pas à se lancer dans la troisième guerre du Vietnam, pourtant lié par une alliance à l'Union soviétique, ce que les Chinois appellent « caresser les fesses du tigre ». Mais le Vietnam, en tentant de dominer le Cambodge et le Laos, aurait créé un pôle de puissance hostile à la Chine en Asie du Sud-Est. Cette guerre contestée est le reflet de la stratégie globale de la Chine. Deng s'éteint doucement à un âge avancé, laissant les fameux messages en quatorze caractères : « Observer avec attention ; traiter les affaires avec calme ; dissimuler nos capacités et prendre notre temps ; savoir user de discrétion ; et ne jamais revendiquer la prééminence » ; le plus secret en douze caractères : « Nous devons être sur la défensive ». Kissinger peut alors décrire la personnalité plus exubérante de Jiang Zemin, l'homme du succès de la Chine.

Vient la conclusion : Kissinger n'est pas partisan de l'ambiguïté. Le message qu'il livre sous le nom de « mémorandum de Crowe » (diplomate britannique qui rédigea, en 1907, une étude sur les risques d'une guerre mondiale avec l'Allemagne) peut être compris comme une mise en garde. La guerre est dévastatrice ; elle est souvent difficile à écarter. Seul un système du monde, accepté et apte à produire ses effets, permet de l'éviter. Il n'y a pas de système du monde sans compréhension mutuelle. La compréhension doit précéder la stratégie car la stratégie et les appareils qu'elle met en place ne sont pas nécessairement inspirés par la compréhension. À méditer alors que le système du monde ne peut exister sans la Chine.

Serge Boidevaix



Bernard Maréchal : **Le Grand jeu sino-américain - Essai sur le devenir du monde** ; Éditions Golias, 2012 ; 170 pages.

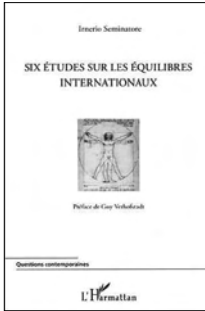
Après avoir lu cet ouvrage on ne pourra pas dire que l'auteur ne prend pas parti. Il ne cache pas son empathie pour la Chine, fondée sur une connaissance profonde et intime de ce pays. Connaissance faite de liens familiaux, de voyages et séjours nombreux et aussi d'une culture impressionnante des bases intellectuelles, économiques et politiques de l'empire chinois. Que le lecteur soit rassuré, il ne s'agit pas d'un exercice de prédiction de l'avenir et en particulier il ne trouvera pas de réponse définitive et péremptoire à la question de savoir si le XXI^e siècle sera le siècle de l'affrontement militaire américano-chinois. En revanche, le lecteur y trouvera une analyse très documentée des ambitions stratégiques chinoises et de ses ressorts historiques, stratégiques, économiques et politiques. Il montre tout au long de son propos combien la montée en puissance de la Chine est inexorable et que si l'hégémonie mondiale n'est pas son ambition, celle-ci n'en reste pas moins décidée à être la puissance dominante en Asie. Ce qui, compte tenu du contexte géostratégique et malgré la connivence économique-financière actuelle avec les États-Unis, la conduit à s'opposer directement à l'Amérique. Dans cette ascension aux extrêmes, la période 2025-2030 devrait être cruciale car elle marquera le début d'une parité militaire avec les États-Unis.

Mais ce livre n'est pas seulement une analyse de ce grand jeu sino-américain, il est aussi un essai sur le devenir du monde et une réflexion sur le devenir de nos démocraties et aussi sur le fait que les zones d'affrontements sont et seront, de façon plus brutale, l'Afrique et l'Asie.

Cette réflexion qui par moments d'ailleurs, prend des allures de digressions hors sujet, apporte peut-être en filigrane la réponse à la question du conflit potentiel sino-américain. En effet cette question serait-elle la bonne ? Les grands mouvements de ce siècle, en particulier la crise économique-financière, le péril environnemental, ne conduisent-ils pas inexorablement à la mise en place de régulations mondiales ; en d'autres termes d'une gouvernance mondiale ? Auquel cas le scénario catastrophe d'une guerre sino-américaine serait la projection d'un scénario inspiré par une vision stratégique passéiste ? Ne faudrait-il pas

plutôt imaginer des scénarios où la Chine serait, de par sa puissance, un acteur global dans un monde global ? Un seul regret cependant, que l'empathie n'occulte le raisonnement. En effet, il semble très réducteur de faire de l'aspiration tibétaine au respect de son identité, un élément de la conspiration américaine à l'encontre de la Chine.

Bernard Norlain

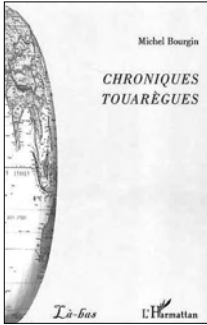


Iinnerio Seminatore : **Six études sur les équilibres internationaux** ; L'Harmattan, 2011 ; 144 pages.

Équilibres certes, mais souvent bien instables ! L'auteur a choisi, à partir de la Renaissance, six périodes ou plutôt autant de « moments-clés » centrés sur la situation politique et stratégique du continent européen, à la fois acteur incontournable et terrain de jeu même si, depuis la Seconde Guerre mondiale, l'établissement d'un ensemble multipolaire et l'entrée en scène des « émergents » ont élargi le théâtre à l'ensemble de la planète et accéléré les évolutions. Le choix du début de la réflexion chez Machiavel, sans retour à l'Antiquité, est assurément raisonnable. Cet homme volontaire et mal aimé, « réaliste désenchanté... logicien impitoyable » a fait ressortir avec bon sens la notion permanente de risque ainsi que le rôle de la force (notamment militaire) et de la ruse. Face à l'éparpillement italien et germanique de l'époque, il a décrit l'État-nation sur le modèle français et espagnol et évoqué le « citoyen-soldat ». Quelque trois siècles après la rédaction de « *Il Principe* », le sage et lucide Metternich, « observateur implacable » recherche au congrès de Vienne, et sans trop d'illusion, le charme du *statu quo*.

Après donc deux premières études consacrées à ces personnages, les quatre autres couvrent la période contemporaine et, négligeant 1918, prennent plutôt 1945 comme point de départ. Elles forment un tout sans découpage chronologique évident, où les dirigeants (Roosevelt, Kennedy, de Gaulle, Adenauer, Obama et Sarkozy) sont plus pilotes que théoriciens. Bien entendu, on retrouve ici, à propos de notre vieux continent, le « dilemme entre intégration et confédération » fusion dans le « sillage atlantique » ou simple Europe des patries ? Les États, où le sentiment national reste enraciné, sont réticents face au « cosmopolitisme ambiant » et consentent à des « transferts de compétence plus que de souveraineté ». Et pourtant, sur l'échiquier planétaire où le foyer principal de puissance se trouve comme toujours en Eurasie et face à l'agitation croissante dans les nouveaux « Balkans mondiaux », dans la perspective aussi d'un relatif déclin américain, la mise en œuvre d'une grande politique eurasiatique basée sur une communauté d'intérêts devient indispensable, alors que nous ne nous trouvons actuellement qu'à mi-parcours. Autant dire que nous rejoignons là la plus brûlante actualité. Si l'appel à l'action est net, si les affirmations sont clairement exposées, la lecture est parfois ardue et réclame une attention soutenue, par exemple lorsqu'il s'agit de distinguer gouvernance et gouvernabilité. Le terme « Étude » indique bien la nature d'un ouvrage destiné, semble-t-il, à un public averti.

Pierre Morisot



Michel Bourgin : ***Chroniques touarègues*** ; L'Harmattan, 2012 ; 364 pages.

Ces chroniques évoquent un peuple. Elles en font revivre les personnalités les plus marquantes (célèbres ou anonymes), les traditions séculaires, les explorateurs, les aventuriers, les religieux, les artistes, les militaires qui ont arpenté le Sahara et le Sahel. Leurs actes anecdotiques ou majeurs ont contribué à la constitution d'une histoire extraordinaire s'apparentant à une chanson de geste, à une saga et « malheureusement parfois, à une tragédie poignante tant le dénouement en est inéluctable ». Cet ouvrage fouillé se présente sous une forme pédagogique : les sujets sont développés et classés par ordre alphabétique. Dans le chapitre consacré à l'origine de ces populations mystérieuses, l'auteur soutient le scénario suivant : un peuple berbère est parti vers l'Est depuis l'Afrique du Nord et le Sahara pour conquérir la Libye et la riche vallée du Nil. Après s'être heurtés aux Égyptiens, « ces grands nomades » ont reçu l'apport de groupes errants venus de la mer, notamment de Philistins dont parle la Bible et plus tard de peuplades balkaniques, pour ensuite se fixer dans la région du Fezzan autour de Garama et, de là, repartir occuper les étendues désertiques de l'Ouest, fuyant la domination des Arabes voulant à leur tour s'installer dans la vallée du Nil. Les *Touaregs*⁽¹⁾ restent avant tout des éleveurs nomades qui vivent de l'entretien de troupeaux de chameaux et de chèvres. Les observateurs retiennent surtout la présence permanente du chameau dont les *Touaregs* connaissent tous les détails du comportement et surtout les énormes possibilités. Le mythique mammifère ruminant constitue la véritable richesse de ces peuples du désert qui entretiennent un véritable lien charnel avec cet « animal noble » : « Pour le *Touareg*, le chameau est sa vie, grâce à lui, il peut se déplacer à son gré dans le désert, faire ses échanges commerciaux, demeurer des mois dans une région sans puits si le pâturage est bon. Le chameau est sa joie, il lui permet de prouver ses qualités d'homme, il est aussi l'objet de ses craintes lorsqu'il est malade ou a disparu après avoir brisé son entrave et qu'il faut le suivre à la trace pendant des jours pour le rechercher ». Jusque dans un passé récent, « le chameau était l'échelle de valeur de la société touarègue où le numéraire était rare. C'était le cadeau approprié pour une naissance ou un mariage ».

Michel Bourgin consacre également une partie captivante aux légendes qui entourent l'imaginaire des *Touaregs*. Ces récits à caractère merveilleux, sublimés par l'invention poétique, sont favorisés par la « majesté et la magie des paysages du désert », ainsi que par les longs moments de solitude qui incitent aux rêveries et développent le goût du surnaturel. Les narrations prenantes mettent en scène un héros, confronté à de

(1) Le terme *Touaregs* est en fait le pluriel de *Targui* (*targuie* au féminin et *targuies* au féminin pluriel). Dans un but de simplification et pour faciliter la compréhension du lecteur, l'auteur a adopté, pour les noms arabes ou *tamachek* (le langage *touareg*), les orthographes les plus couramment utilisées dans les ouvrages traitant du Sahara.

mauvais génies hantant des sommets ou des cavernes inaccessibles, qui reçoit l'aide de bonnes fées vivant habituellement sous la forme de gazelle ou de petit oiseau. Les légendes abondent dans la culture touarègue. La plupart exaltent, pour mieux les transmettre, des valeurs fondamentales comme le courage, la loyauté et l'amour.

L'histoire des *Touaregs* est intimement liée à l'aventure coloniale française et à l'âge d'or des explorations des géographes, des scientifiques et des idéalistes. Les plus chanceux revinrent de leur folle entreprise dans la plus vaste zone désertique du monde pour récolter la célébrité. Ce fut le cas de René Caillié (1799-1838), le premier Européen revenu vivant de « Tombouctou la Mystérieuse » en 1828 et d'Henri Duveyrier (1840-1892) qui séjourna plus d'une année chez les *Touaregs* des Ajjer (1860-1861) dans un massif montagneux au nord du Hoggar. Ce périple alimenta la trame de son livre, *Les Touaregs du Nord*, écrit avec le docteur Warnier (1864), un ouvrage qualifié par l'auteur de « chef-d'œuvre qui est fondamental pour la connaissance du Sahara et surtout de celle des *Touaregs* ». Le destin de Charles de Foucauld (1858-1916), qui a consacré douze années de sa vie aux *Touaregs* dont il fut l'ami, fait aussi l'objet d'une longue réflexion. L'explorateur et missionnaire, qui a donné son nom à une promotion de Saint-Cyr (1941-1942), a laissé à la postérité des témoignages écrits sur la civilisation de ces vagabonds des sables qu'il a intimement côtoyés, ainsi qu'une grammaire et un dictionnaire *Touareg-Français*. Dans ce registre de la présence française au Sahara, Michel Bourgin relate également le parcours d'un autre saint-cyrien, Henry Laperrine (1860-1920), qui pacifia les territoires des oasis et créa les légendaires compagnies sahariennes. Dans cet historique passionnant figure aussi le programme du « Transsaharien », né dans les esprits après la défaite de 1870, à une époque où la France cherchait « une action susceptible de fédérer ses énergies tout en retrouvant de l'audience dans le concert européen ». Mais le projet de ce long ruban d'acier devant relier la Méditerranée au Niger disparaîtra avec la fin de la colonisation.

Le document du général (2S) Bourgin, ancien président de la Société de géographie de Tours et actuellement membre de la Société de géographie de Paris, présente un intérêt évident, d'ordre essentiellement culturel, en ce sens qu'il plonge le lecteur dans les tréfonds de la civilisation touarègue. Cette étude est d'autant plus fascinante qu'elle s'appuie sur quelque quatre-vingts ouvrages de référence cités en bibliographie et qu'elle remet au goût du jour des débats qui touchent à l'histoire saisissante de l'action (souvent mal comprise) de la France au Sahara.

Michel Klen

Revue Défense Nationale

COMITÉ D'ÉTUDES DE DÉFENSE NATIONALE

■ CONSEIL D'ADMINISTRATION

- MM. l'Amiral A. COLDEFY, *président*.
Y. BOYER, professeur à l'École polytechnique, président de la Sfem, *vice-président*.
D. JOUAN, ingénieur général de l'armement, *trésorier*.
B. d'ABOVILLE, ambassadeur.
A. BAUER, professeur de criminologie au Cnam, président du CSFRS.
le général d'armée Th. CAMBOURNAC, inspecteur général des armées (Terre).
P. CHAIGNEAU, administrateur général du Centre d'études diplomatiques et stratégiques.
B. DURIEUX, inspecteur général des finances, ancien ministre.
Th. GARCIN, maître de conférences à HEC, producteur délégué à Radio-France.
A. JUILLET, Conseiller senior au Cabinet Orrick Rambaud Martel.
le vice-amiral d'escadre R. LABORDE, directeur de l'IHEDN et de l'EMS.
le général d'armée aérienne J.-P. MARTIN.
L.-F. SALVADOR, président-directeur général Groupe Sogeti.
G.-H. SOUTOU, membre de l'Institut.
le général d'armée M. WATIN-AUGOUARD.

■ PRÉSIDENTS ET VICE-PRÉSIDENT D'HONNEUR

- MM. le général d'armée aérienne B. NORLAIN.
le général d'armée C. QUESNOT.
le général d'armée aérienne Ph. VOUGNY.
Cl. CONTAMINE.

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

Secrétaire général : Jacques Mourgeon - Tél. : 01 44 42 43 72

Rédacteur en chef : Jean Dufourcq - Tél. : 01 44 42 31 90

Rédacteur en chef de l'édition anglaise : Mike Storey - Tél. : 01 44 42 31 90

Rédacteur en chef de l'édition russe : Olivier Védrine - Tél. : 01 44 42 31 90

Rédacteur en chef de l'édition arabe : Fadi Assaf - Tél. : 01 44 42 31 90

Secrétaire général de rédaction : Pascal Lecardonnel - Tél. : 01 44 42 31 90

Assistante de direction : Marie-Hélène Mounet - Tél. : 01 44 42 31 92

Secrétaires de rédaction : Marie-Hélène Mounet, Jérôme Dollé, Umera Haji, Joseph Hokayem, Fabrice Renouard

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

Administration du site *Internet* : Paul Laporte - Tél. : 01 44 42 31 91

Conseiller de rédaction : Olivier Kempf

Régie publicitaire : BKSM Advertising - Tél. : 01 56 99 71 73

DL 78380 - 2^e trimestre 2012 - ISSN : 2105-7508 - CP n° 1014 G 85493 du 9 septembre 2010

Imprimée par Bialec, Nancy, 95 boulevard d'Austrasie, BP 10423, 54001 Nancy cedex

Le comité de lecture : F. Blachon, Y. Boyer, R. Carmona, Pr. P. Chaigneau, A. Dumoulin, A. Hervey, C. Le Borgne, S. de Maupeou, B. Norlain, P. d'Ornano, C. Revel, Pr. A. Sedjari.

NOS POINTS DE VENTE EN FRANCE

● LIBRAIRIES EN ÎLE-DE-FRANCE ●

Librairie Galignani - 224 rue de Rivoli, Paris 1^{er}
Librairie Julliard - 229 bd Saint-Germain, Paris 7^e
Librairie Sciences politiques - 30 rue Saint-Guillaume, Paris 7^e
Librairie de l'École militaire - 41 av. de La Motte-Picquet, Paris 7^e
La Documentation Française - 29/31 quai Voltaire, Paris 7^e

● GARES ET AÉROPORTS - RELAIS H ●

Gare du Nord, voies 3 et 13, Paris 10^e
Gare d'Austerlitz, vestibule B, Paris 13^e
Gare Montparnasse, grandes lignes, Paris 14^e
Orly Ouest, n° 402, hall 2

● LIBRAIRIES EN PROVINCE ●

Librairie Privat - 14 rue des Arts, 31000 Toulouse
Librairie Dobrée - 14 rue Voltaire, 44000 Nantes
Maison de la Presse - 3 rue Albert Jacquemin, 88120 Vagney
Roche diffusion Presse - Rue des Bazinières, 85006 La Roche-sur-Yon
Vosges Diffusion Presse - BP 92 - 2 allée des Maronniers, 88192 Golbey cedex

Votre libraire souhaite devenir dépositaire de la RDN - © 01 44 42 38 23

CAHIER DES CHARGES AUTEURS

Le Comité d'études de défense nationale sollicite des articles rédigés en français, inédits, et selon le protocole éditorial suivant :

- Pour les rubriques « Thématiques », les textes comprendront de 15 000 à 20 000 signes et seront référencés à des sources apparaissant en notes dans la page.
- Pour les rubriques « Repères/Opinions/Débats » et « Tribune » (*Internet*), les thèses ou points de vue se limiteront entre 10 000 et 12 000 signes accompagnés d'une éventuelle bibliographie d'appui renvoyée en fin de texte. Une biographie d'environ 200 signes est à fournir pour ces rubriques.

- Pour les « Revues » qui offrent un panorama stratégique national et international, et les « Rapports », qui exposent une étude ou une recherche spécifique, les textes ne doivent pas excéder 5 000 signes. Pour les « Recensions » qui exposent le contenu d'un ouvrage et l'opinion du rédacteur, les textes ne doivent pas dépasser 3 000 signes.

Les articles soumis à publication doivent être envoyés pour évaluation au comité de lecture de la rédaction par courrier électronique (redac@defnat.fr). Le contenu du texte et les références restent de la responsabilité exclusive des auteurs et les opinions émises n'engagent pas la RDN. Les droits de traduction, reproduction et d'adaptation sont réservés pour tous pays. Les auteurs francophones, doctorants, jeunes chercheurs en affaires stratégiques, officiers de l'enseignement militaire supérieur font l'objet d'une attention particulière du comité de lecture. Les règles de rédaction et de référencement sont celles de l'Imprimerie nationale. Tous les textes qui ne correspondraient pas aux critères linguistiques standards et aux exigences de rigueur critique seront renvoyés aux auteurs pour adaptation avant évaluation par le comité de lecture. La publication des textes évalués reste subordonnée à des ajustements éventuels de forme ou de fond. À l'issue du processus d'approbation, un résumé en français et en anglais est établi. L'auteur d'un article en réserve l'exclusivité à la RDN et s'engage à ne le développer ou le résumer sans faire mention de la RDN.

Le « bon à tirer » vaut cession de droit et autorise le CEDN à publier un article sur supports papier ou sur l'*Internet*. En contrepartie, l'auteur bénéficie d'un abonnement de 6 mois à la RDN à compter du mois de la parution de son article (tous numéros supplémentaires lui seront facturés). Une épreuve numérique de son article peut lui être envoyée par courriel sur simple demande.



Quelle Revue Défense Nationale voulez-vous en 2013 ?

Mensuelle : 10 numéros par an
Bimestrielle : 6 numéros par an
Trimestrielle : 4 numéros par an

Donnez-nous votre avis
sur

www.defnat.com
ou contact@defnat.com

Si vous n'avez pas accès à l'*Internet* pour compléter le questionnaire, photocopiez et retournez-nous cette page. Nous en tiendrons compte.

- Formule mensuelle (152 pages) : augmentation des tarifs de vente.
- Formule bimestrielle (160 pages) : maintien des tarifs 2012.
- Formule trimestrielle (184 pages) : maintien des tarifs 2012.

Nom _____ Prénom _____

Date de naissance _____ Profession _____

Adresse _____

Des articles inédits chaque semaine sur la « Tribune » *Internet*

LES DERNIÈRES PARUTIONS

Alain-Roger Mvelle : « De la négation du champ politique comme théâtre de la guerre civilisée en Afrique : leçons du cas malien I » ; *Tribune* n° 201, 11 avril 2012.

Le récent coup d'État militaire au Mali inspire à l'auteur cette analogie entre le champ politique – et sa militarisation – et le champ de bataille. Il invite à revenir aux règles de la guerre civilisée.

Abdou Ibro : « Conséquences économiques et sécuritaires des transitions maghrébines sur le Niger : essai d'analyse prospective » ; *Tribune* n° 202, 12 avril 2012.

Une première approche structurelle révèle les vulnérabilités qu'induit au Niger la transition maghrébine.

Pierre Lacoste : « Sur la géostratégie du crime » ; *Tribune* n° 203, 13 avril 2012.

Le récent ouvrage qui traite de la géostratégie du crime inspire à l'auteur cette réflexion sur la permanence et l'adaptation constante des structures du crime organisé qui ont colonisé les États et enrôlent désormais dans leurs entreprises des acteurs multiples.

Claude Le Borgne : « Le soldat Montaigne » (en 3 parties) ; *Tribunes* n° 204, 17 avril 2012, n° 213, 9 mai 2012 et n° 215, 15 mai 2012.

L'auteur, qui s'y amuse, relit les *Essais de Montaigne* et révèle l'homme de guerre. Leçons pour ceux d'aujourd'hui.

Guirec Doniol : « Le fait aérien dans la Marine » ; *Tribune* n° 205, 18 avril 2012.

Voir loin, observer, se repérer, obsession du marin ; s'élever pour voir derrière l'horizon, le souci du militaire. L'Aéronautique navale en procède directement.

Jean Dufourcq et Fabrice Renouard : « Du consensus de défense nationale en 2012 » ; *Tribune* n° 206, 24 avril 2012.

La rédaction de la RDN fait un bilan succinct du quinquennat et esquisse les bases d'un nouveau consensus de défense que l'on peut dégager à la lecture des programmes de défense des cinq principaux candidats à l'élection présidentielle.

Emmanuel Dupuy : « “Quel avenir pour la Libye ?” » ; *Tribune* n° 207, 25 avril 2012.

Les principaux défis qu'affronte la Libye depuis l'effondrement du régime Kadhafi mettent en cause son identité, son unité, sa viabilité. La question tribale est au cœur du pouvoir et conditionne l'avenir du pays.

François Hollande : « La défense nationale demain » ; *Tribune* n° 208, 26 avril 2012.

Nicolas Sarkozy : « Défendre la France » ; *Tribune* n° 209, 26 avril 2012.

Amin Hoteit : « Syrie : conséquences de la résolution 2042 » ; *Tribune* n° 210, 2 mai 2012.

Cette analyse engagée de la résolution 2042 montre la complexité actuelle d'un pays en proie à la fois à des menées contestataires internes et à une manœuvre extérieure de changement de régime.

Florent Khing : « Le couple militaire-humanitaire : “je t'aime, moi non plus...” » ; *Tribune* n° 211, 3 mai 2012.

L'indispensable coopération entre militaires et humanitaires peut encore être améliorée en situation de crise, notamment par la valorisation d'instances de coordination et une répartition plus claire des rôles de chacun.

Markus Kafurke : « Penser “interarmées” au sens large dans le domaine de l'armement » ; *Tribune* n° 212, 4 mai 2012.

Le cadre des opérations militaires a beaucoup changé depuis la fin de la guerre froide. En revanche, le développement des armements a peu évolué. Une meilleure connaissance mutuelle entre les armées, la DGA et les entreprises civiles peut permettre d'économiser du temps et de l'argent pendant le développement des programmes d'armements.

Laurent Paccaud : « Athéna : chronique d'une mort annoncée » (en 2 parties) ; *Tribunes* n° 214, 10 mai 2012 et n° 217, 16 mai 2012.

Le financement des coûts communs des opérations et notamment celui de leur démarrage est une condition essentielle de leur efficacité. Faute d'avoir pu se positionner correctement dans la structure du Conseil et d'avoir développé des bonnes pratiques opérationnelles suffisantes, le mécanisme Athéna va périlcliter et entraver de fait la dynamique de la PCSD.

Jean Dufourcq : « La Méditerranée de demain : enjeux et défis vus de Tunis » ; *Tribune* n° 215, 11 mai 2012.

C'est à une radiographie de la Méditerranée au filtre de la transition politique tunisienne que se livre l'auteur. Il rend compte des travaux conduits récemment pour mettre en perspective les changements en cours en Afrique du Nord. Le sentiment qui domine est une urgence économique et sociale que la réforme politique peine à prendre en charge.