Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Service d'information du Gouvernement

Livres *d'actualité*

Pour une stratégie globale de sécurité nationale

PRESAJE

sous la direction de
Nicolas Arpagian et Éric Delbecque

préface de
Alain Bauer

DALLOZ – 2008

N° 318 / JUILLET 2008

LIVRES D'ACTUALITÉ présente, chaque mois, un certain nombre de notes de lecture d'ouvrages apportant un éclairage sur les mouvements d'idées, les tendances qui se dessinent en ce début de XXIe siècle.

DÉPARTEMENT RESSOURCES D'INFORMATIONS : Tél. : 01 42 75 78 23
LYDIE GORDEY : Tél. : 06 33 53 18 39 - Mél. : lydie.gordey@free.fr

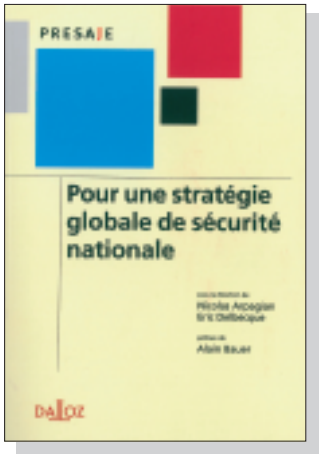
Pour une stratégie globale de sécurité nationale

PRESAJE*

sous la direction de Nicolas Arpagian et Éric Delbecque**

préface de Alain Bauer***

Le plus souvent, en matière criminelle ou terroriste, ce qui est nouveau, c'est ce qu'on a oublié, écrit Alain Bauer en préface à l'ouvrage. Il poursuit : entre ce qu'on sait, ce qu'on croit et ce qu'on cherche, ce qu'on sait est hélas la plus petite partie de l'ensemble. En matière criminelle, Conan Doyle fait dire à Sherlock Holmes que ce qui reste, une fois l'impossible supprimé, doit être la vérité, même si c'est incroyable. Or, avant le 11 septembre, en matière de terrorisme, ce qui est incroyable était supposé impossible… Et l'incroyable est devenu réalité. Depuis la chute du mur de Berlin, les frontières et les espaces ont changé. Le crime comme le terrorisme ont appliqué les lois du libéralisme économique et de la globalisation. Les entreprises criminelles sont devenues des entreprises comme les autres. Si l'Europe du crime est déjà faite, l'Europe de la police et de la justice reste à faire. Si le monde du crime est déjà globalisé, seule sa police reste morcelée. Voici pourquoi la reconstruction d'une pensée stratégique est un passage obligatoire. Passer de la Défense globale à la Sécurité globale, prendre en compte les entreprises comme sujet stratégique, au-delà même de leur outil de production, intégrer la dimension virtuelle de nouveaux risques et de nouveaux conflits, ouvrir le champ au décèlement précoce et à l'anticipation, voici les enjeux de la redéfinition de l'espace stratégique français. La sécurité nationale est assurément une des missions essentielles de l'appareil d'État. Toutefois, elle ne peut désormais s'envisager sans prendre en compte les trois autres intervenants que sont l'opinion publique, le secteur privé de la défense et l'échelon politique européen, concluent Nicolas Arpagian et Éric Delbecque. C'est la raison pour laquelle la sécurité nationale ne peut plus se concevoir dans le seul cadre traditionnel d'un ministère de la Défense. Puisque la menace est polymorphe, les réponses – et ceux qui travaillent à les élaborer et à les mettre en place – doivent émaner d'horizons divers. La France vient de se doter d'un Livre blanc visant à bâtir sa stratégie de sécurité nationale pour la quinzaine d'années à venir. Cette sécurité nationale exige des investissements humains, matériels et financiers lourds, car les hommes et les équipements doivent être immédiatement opérationnels en cas de crise, et permettre également d'anticiper au mieux lesdites crises. Seul un climat général de confiance dans la sécurité d'un État rend possible les investissements permettant sa prospérité économique. C'est de cet équilibre, entre sécurité du cadre de vie et dynamisme des entreprises, que naît la construction d'un possible collectif. Il n'y aura pas de croissance durable sans au préalable des investissements conséquents dans le champ de la défense et de la sécurité nationales.



2008 - 304 pages - 32 €

* *L'institut PRESAJE* – Prospective, Recherche et Études sociétales appliquées à la Justice et à l'Économie – *est un* "Think Tank" *indépendant, dédié à l'analyse des relations complexes entre l'économie, le droit et la justice.*

** *Nicolas Arpagian, rédacteur en chef de la revue* Prospective Stratégique, *enseignant à l'Institut d'Études et de Recherche pour la Sécurité des Entreprises (IERSE), est l'auteur de* Liberté, Égalité… SÉCURITÉ *(Dalloz, 2007).*

Éric Delbecque, secrétaire général de l'IERSE, est l'auteur de Quel patriotisme économique ? *(PUF, 2008).*

*** *Alain Bauer, criminologue, est président du Conseil d'orientation de l'Observatoire national de la délinquance, et président de la Mission sur le rapprochement des institutions de formation et de recherche sur les questions de sécurité et stratégiques (présidence de la République et Premier ministre). Il a publié* Géographie de la France criminelle (Odile Jacob, 2006).

La place du renseignement dans la politique de sécurité nationale

*Rémy Pautrat**

Une politique publique de renseignement forme le socle même d'une stratégie de sécurité nationale. Car aujourd'hui, plus que jamais, il faut *savoir* pour *agir* efficacement et adroitement. Pourtant, le monde du renseignement souffre toujours d'un manque singulier de considération propre à notre pays. Pour un certain nombre de nos contemporains, y compris parmi les décideurs politiques et la haute administration, le renseignement apparaît essentiellement contraire à l'esprit de la modernité libérale et démocratique. Malheureusement, entre les idéaux infiniment respectables de la modernité et la réalité de la scène géopolitique et géoéconomique mondiale, il existe un gouffre important fait de toute une gamme d'acteurs qui n'ont pas renoncé à l'exercice de la violence comme outil politique. Il faut donc en tirer les conséquences nécessaires : à savoir que les services de renseignement sont les seuls instruments que nous pouvons utiliser pour connaître nos adversaires réels et pouvoir ensuite déterminer les moyens nécessaires à leur affaiblissement.

Le premier rôle du renseignement ? Identifier l'ennemi. En effet, aujourd'hui pour la première fois depuis dix siècles, *l'ennemi ne va pas de soi*… Les gouvernements se trouvent donc confrontés à une lourde difficulté : celle de ne pas céder à la facilité et à l'émotion populaire relayée par la puissance médiatique. Car il est effectivement commode, pour le pouvoir comme pour les médias, de disposer d'un ennemi clair et imposant. Si on échoue à le trouver, il est tentant d'en construire un de toute pièces.

La nature même de l'ennemi possible pose donc problème. Celui-ci n'est plus un État solide, puissant, organisé, centralisé, adossé à des armées, des administrations, des territoires… L'ennemi d'aujourd'hui est furtif, instable, ductile, organisé en réseaux et s'appuyant sur quelques centaines ou milliers d'hommes éparpillés. Il ne vise pas à vaincre par le nombre et la puissance de feu, ou même la contagion idéologique spontanée, mais par le choc médiatique, la sidération, l'émotion collective. Ce qu'il faut également prendre en considération, c'est la plasticité idéologique du phénomène et la résolution forte qui en découle… Celui qui veut vraiment donner la mort déploiera des trésors d'inventivité pour mettre en oeuvre sa logique de terreur.

On voit bien que dans une telle configuration, il ne sert pas à grand-chose de s'enfermer dans une pathologie sécuritaire qui se révèle tout simplement intenable sur le long terme. Il paraît en revanche plus utile de développer une politique de renseignement capable de saisir les modes de fonctionnement de cet ennemi *infra-étatique* dont le modèle d'organisation appartient à l'ère du monde en réseaux. Mais le terrorisme n'est pas le seul enjeu sur lequel doit travailler le monde du renseignement. Ce dernier a également pour mission de contribuer à la défense des intérêts essentiels, vitaux, de la nation. Or, notre puissance économique participe de ces intérêts.

Renseignement et sécurité économique. Ce qu'il faut bien comprendre, c'est qu'à la confrontation idéologique Est-Ouest a succédé une ère qui se caractérise par une diversification des facteurs de conflit et par le basculement d'une partie des affrontements de la sphère géopolitique à la galaxie des rivalités géoéconomiques. La violence de ces phénomènes modifie en profondeur les formes de pouvoir, et consacre l'information au rang de *matière première stratégique*. Or cela signifie une exigence de tout instant, car il faut tout à la fois accroître nos capacités coopératives et nos savoir-faire en matière de concurrence. De nouvelles règles du jeu se mettent en place où *partenariat et concurrence* se disputent simultanément le terrain.

Dans le domaine de la gestion stratégique de l'information utile aux acteurs économiques, la France ne sait pas encore tirer le meilleur de la "société de l'information" qui régit le monde de l'après Guerre froide. C'est pourtant un enjeu de savoir, de connaissance et donc de pouvoir, de première importance.

Il est en effet essentiel que nous soyons en mesure de faire prévaloir deux impératifs en matière de protection de notre substance informationnelle économique :

- La défense du périmètre stratégique de souveraineté, c'est-à-dire la défense des entreprises sensibles participant des secteurs stratégiques récemment définis par le gouvernement (sécurité, biotechnologies, production d'antidotes, matériel d'interception et de communication, technologies duales, marchés secret défense, armement…).
- La diffusion d'une culture de la sécurité du patrimoine informationnel et productif au sein des entreprises. Pour l'entreprise, la difficulté d'un tel exercice réside dans l'aptitude à trouver le juste équilibre entre circulation de l'information et protection de la connaissance stratégique au cœur de l'avantage concurrentiel.

La stratégie américaine. De ce point de vue, l'exemple américain est emblématique. Dès son arrivée au pouvoir, le président Clinton s'était investi quotidiennement dans la promotion des intérêts économiques de son pays dans le monde. En 1992, il avait créé à cet effet le *Conseil économique national* – NEC – qui lui était directement rattaché et avait pris une importance comparable à celle du *Conseil national de sécurité*. Réuni régulièrement sous son autorité, le NEC conseillait en particulier le Président sur les orientations de la diplomatie économique, dont les entreprises françaises vivent chaque jour la réalité de l'efficacité sur les marchés européens et internationaux.

En France, la démarche de *sécurité économique* est un concept récent dont l'application ne fait que commencer. La sécurité économique est l'autre nom d'un projet et d'une politique d'accroissement de puissance économique. Seule la proximité (ce qui ne veut pas dire collusion ou complaisance) entre le politique et l'appareil de renseignement permet de nos jours de nourrir la diplomatie et la stratégie globale d'influence dont notre pays a besoin. Proximité qui se révélera d'ailleurs le plus sûr moyen d'éviter les "dérapages" que provoque naturellement le fait que les services spécialisés soient livrés à eux-mêmes pour définir leurs propres missions.

La coordination du renseignement. Elle pourrait se manifester *via* un *coordonnateur* du renseignement, membre du conseil de sécurité nationale. Avec les directeurs des grands services qui concourent au recueil et à l'exploitation du renseignement, le coordonnateur animerait la communauté du renseignement et veillerait à entretenir un esprit de cohésion et à renforcer la volonté d'action collective. Il n'aurait aucune autorité hiérarchique sur les services. Il lui appartiendrait, en revanche, d'attirer l'attention sur le besoin d'une concertation interministérielle lorsque les informations dont il disposerait le justifieraient. Il serait entouré d'une équipe légère de professionnels du renseignement et des relations internationales. D'une manière générale, le coordonnateur devrait garantir le bon fonctionnement et l'efficacité de la communauté du renseignement, au service des autorités responsables de la décision et de l'action. Il élaborerait des synthèses de renseignement pour le Chef de l'État, le Premier ministre et les membres du Gouvernement. Il prêterait, également, un soin particulier à la circulation rapide du renseignement ou de l'information utile. Cet état d'esprit est fondamental dans le domaine économique, scientifique, technologique et commercial.

** **Rémy Pautrat**, préfet honoraire de région, a notamment été directeur de la DST (1985-1986) avant de devenir conseiller technique puis conseiller pour la sécurité auprès du Premier ministre. Préfet de la région Basse-Normandie en 1996, il imagina le premier schéma régional d'intelligence économique. Il est actuellement délégué général de France Intelligence Innovation.*

Cyberconflits, ou comment les technologies de l'information réécrivent l'Art de la Guerre

*Nicolas Arpagian**

La journée du 26 avril 2007 restera-t-elle comme une date-clé dans l'Histoire militaire mondiale ? C'est en effet ce jour-là, à vingt-deux heures trente, qu'a été enregistrée la première agression informatique concertée contre les institutions politiques, gouvernementales, économiques et même médiatiques d'un pays. En l'espèce, il s'agit de l'Estonie, dont les sites Internet des principales banques, des organismes gouvernementaux, de plusieurs organes de presse… ont été saturés par des envois massifs et simultanés de courriers électroniques, afin d'empêcher toute connexion. Cette manière de faire, dite attaque DDOS (pour *Distributed Denial of Service*), est une première dans son genre. Il s'agissait de paralyser tout le fonctionnement d'une nation. L'origine précise de ce raid numérique n'a pas été formellement établie, même si des rumeurs convergentes évoquaient une piste remontant aux autorités russes.

Les nouvelles armes de la guerre électronique. À la fin novembre 2006, la Commission états-unienne d'étude économique et de sécurité sur la Chine *(US-China Economic and Security Review Commission)* s'est inquiétée très officiellement dans un rapport qu'elle a remis aux présidents du Congrès et de la Chambre des Représentants du fait que Pékin ait mis en place des unités spécialisées dans le combat cybernétique. Leur rôle serait clairement, selon cette commission, de concocter des virus informatiques capables de pénétrer les défenses numériques des États-Unis. Voire de paralyser par ce biais ses systèmes financiers.

La guerre médiatique. Alors que des campagnes militaires de grande envergure supposent des effectifs nombreux, formés, équipés avec en outre d'importants moyens logistiques pour assurer leur déploiement, les cyberconflits ont effectivement pour eux de ne mobiliser que l'imagination et la créativité de quelques cerveaux d'experts ès-SIC (systèmes d'information et de communication).

Effet indéniable de l'avènement de cette société de l'information : la guerre médiatique fait, elle aussi, partie intégrante de la manière dont doit désormais s'envisager un conflit armé. Alors que les attentats étaient longtemps revendiqués par l'envoi de messages à des rédactions, aujourd'hui c'est directement *via* des sites Internet amis que les organisations terroristes formulent leurs prises de position.

De nouveaux outils de contrôle. Au cœur de l'été 2007, le gouvernement chinois a annoncé le déploiement de policiers virtuels pour patrouiller sur Internet. Présentés sous la forme de petits personnages de dessin animé, ils apparaissent désormais toutes les demi-heures sur les écrans des internautes connectés à des sites installés à Pékin. Histoire de leur rappeler qu'ils sont toujours sous surveillance, notamment qu'ils se rendent sur "les sites jugés nocifs". Faculté supplémentaire : il est possible de signaler à la police des contenus que l'on considère suspects. La politique de sécurité se trouve amplifiée et confortée par ces mécanismes informatiques, au point d'en faire des auxiliaires majeurs de l'instauration d'un contrôle des populations.

Durant ce même été 2007, le Congrès américain a donné son accord pour l'entrée en vigueur d'un programme d'écoute électronique sans mandat

judiciaire préalable. Le 4 août 2007, la Chambre des Représentants a ainsi voté une modification du *Foreign Intelligence Act*, autorisant l'Administration états-unienne à intercepter les communications électroniques ou téléphoniques des ressortissants étrangers de passage sur le territoire des États-Unis. Seul bémol : un mandat judiciaire est nécessaire si c'est un ressortissant américain qui est la cible des écoutes.

Dans le même esprit, Washington a communiqué, en octobre 2007, le lancement d'un nouveau programme du *Department of Homeland Security,* baptisé "CyberInitiative". En mettant à contribution la *National Security Agency* (NSA) et le FBI, il s'agira de prolonger le dispositif *Turbulence* qui vise à assurer la sécurité des infrastructures informatiques gouvernementales et militaires. Avec, et c'est là que réside la nouveauté, l'intention d'élargir cette protection aux équipements des entreprises et des particuliers, afin d'éviter les contaminations en chaîne.

Face à un tel déferlement informatique, l'Union européenne ne pouvait rester sans rien faire. Et voilà donc, en octobre 2007, que la Commission, par la voix de Viviane Reding, la commissaire en charge de la société de l'information, a annoncé la création d'une unité spéciale, chargée de protéger les réseaux électroniques de l'UE. Il s'agirait d'un département au sein de la future Autorité européenne des télécommunications (ETMA), qui doit voir le jour le 1er janvier 2010.

Vers la numérisation de l'espace de bataille. "C'est une remise en cause de l'organisation telle qu'elle datait de Napoléon." C'est par cette formule lapidaire qu'un officier général définissait, fin 2007, à un public d'industriels le concept que les militaires français apprennent à connaître depuis 2003 : la NEB – pour *Numérisation de l'Espace de Bataille*. Il s'agit de la traduction à la française du concept états-unien de *network-centric warfare* ou opérations en réseau, qui a émergé au début des années 90. Tout le monde disposant au même moment de la même information, cela limite considérablement, par exemple, les risques de tirs fratricides, et assure une meilleure réactivité face aux inévitables aléas des interventions ennemies. En l'espèce, cet apport technologique permet un réel travail collaboratif, et renforce donc les échanges entre les individus.

Question calendrier : le ministère français de la Défense annonce pour 2009 la mise en place de forces numérisées aptes au combat. Et prévoit "vers" 2015 la numérisation de l'ensemble des forces terrestres projetables.

Seule certitude : cette multiplication d'outils électroniques va susciter des besoins nouveaux et croissants. Et certainement créer des vulnérabilités supplémentaires. Lorsque l'on place ses espoirs dans la technologie pour assurer sa sécurité, les pistes de développement semblent infinies. Le Congrès des États-Unis a demandé à la DARPA (*Defense Advanced Research Projects Agency)* de faire en sorte qu'en 2015, un tiers des véhicules de l'US Army soient utilisables sans pilote. Une perspective que la revue française *Heraclès* résume à sa manière : "Le plus vieux métier du monde ne doit pas être archaïque."

La sphère privée. Pas question, pour l'auteur, de verser dans un optimisme béat qui verrait dans les technologies de l'information et de la communication le meilleur moyen de sécuriser un monde de plus en plus instable. Ni dans une paranoïa, destructrice à la longue, qui assimilerait forcément lesdites technologies à des outils d'asservissement de l'individu. La sécurité nationale étant assurément un bien commun qu'il faut préserver, il serait, conclut-il, souhaitable que les Français aient une vision la plus claire possible de ces questions qui conditionnent pour l'avenir la longévité de la société dans laquelle ils ont une chance de s'épanouir et de vivre en bonne intelligence. Cela s'appelle tout simplement la démocratie.

* ***Nicolas Arpagian,*** *rédacteur en chef de la revue* Prospective Stratégique*, enseignant à l'Institut d'Études et de Recherche pour la Sécurité des Entreprises (IERSE), est l'auteur de* Liberté, Égalité… SÉCURITÉ *(Dalloz, 2007).*

L'influence : un outil de sécurité nationale

*François-Bernard Huyghe**

La notion d'influence recouvre à la fois :

- La faculté psychologique de convaincre, de susciter l'imitation, de changer un comportement ;
- une catégorie sociologique (l'influence des médias, des intellectuels, des groupes ou réseaux dits justement d'influence…) ;
- mais c'est aussi une forme politique de pouvoir, et donc un instrument de sécurité nationale (qui n'est pas du ressort des relations d'autorité, de violence ou de contrat, et qui néanmoins fait agir les hommes).

C'est même une méthode géopolitique. L'influence s'oppose alors à la puissance, en tant que capacité propre à certains acteurs internationaux de gagner un soutien ou une approbation hors de leurs frontières, ou de peser sur la décision d'un autre acteur. En théorie, il existe plusieurs méthodes d'influence, dont aucune ne peut se trouver à l'état chimiquement pur ; elles se mêlent toujours à un degré ou à un autre.

Rayonner. L'influence est alors affaire de prestige. En France, nous aimons nous considérer comme le pays des droits de l'homme, du multilatéralisme, de la culture, de la qualité de vie, etc., et avons trop souvent tendance à ne compter que sur cet atout. Cela peut provoquer un agacement chez nos

partenaires : personne n'a envie d'acheter des TGV à notre pays parce que c'est celui de Molière, ni d'y faire les Jeux Olympiques de 2012 parce qu'il fait vanter par Deneuve et Depardieu les charmes de Paris dans un film.

Persuader. La persuasion mobilise des techniques pour faire adhérer un sujet à une affirmation, vraie ou fausse. Il s'agit de faire parvenir des mots convaincants ou des images séduisantes à une population cible. Encore faut-il que les messages trouvent des récepteurs prédisposés.

Contrôler. La stratégie du message appelle aussi une stratégie du vecteur. La prolifération des chaînes internationales d'information multilingues en fournit un excellent exemple.

Formater. Ce stade peut prolonger les deux précédents. Il s'agit de jouer sur les codes mentaux, les catégories qu'emploient les gens, les termes dans lesquels ils pensent la réalité.

Inspirer. C'est une technique plus subtile encore. Elle agit très en amont sur le processus de décision ; l'idée voyage de tête en tête, se trouve traduite, adaptée et réappropriée à chaque étape. *Think Tanks,* ONG, lobbies affirment ainsi leur emprise par de simples vocables repris par les médias et par la classe *discutante*. Inventer la notion de développement durable, de guerre préemptive ou de droit opposable au logement : voilà une forme indéniable de l'influence. Mais il ne suffit pas de produire, il faut aussi "distribuer" : combiner une cosmétique (bien présenter les idées), une balistique (bien les faire parvenir à leur cible) et une logistique (user des bons moyens).

Agir en réseau est sans doute la forme la plus commune et la plus évidente de l'influence. C'est un mode d'action politique sur et par l'opinion. Parallèlement, une notion s'impose avec le développement d'Internet : celle de réseaux sociaux. Ce quasi-pléonasme renvoie à la faculté qu'offre le Net de créer des relations instantanées, de produire du commentaire et de l'évaluation incessants sur tout, depuis le gadget jusqu'à des questions de politique internationale.

Influence, désordre et chaos. En tant que stratégie indirecte utilisant des signes et symboles pour peser sur les décisions d'autrui, l'influence peut viser, non seulement à séduire et concilier, mais aussi à déstabiliser.

En temps de Guerre froide, l'agent d'influence apparaissait comme le plus subtile et le plus subversif des agents secrets. Aujourd'hui, les officines d'influence oeuvrent plutôt dans la *désinformation* ou la *déstabilisation économique*. Le lancement d'une rumeur économique ou l'instrumentalisation de la dénonciation par les ONG deviennent des armes de la guerre économique. Parallèlement, la *contre-influence*, ou art de se préserver des attaques informationnelles, se développe aussi bien en intelligence économique que dans les pratiques politiques et joue un rôle crucial dans une perspective d'anticipation ou de gestion de crise.

ACM. Cette notion prend de l'importance dans les années 90 : c'est celle d'*affaire, action ou coopération civilo-militaire*. Elle est liée à des conflits typiques de la fin du XX^{e} siècle : des États disloqués, en proie à des guerres civiles, ou des situations indécises entre guerre et paix. Chaque État mène les ACM avec sa méthode, voire sa doctrine. La France, impliquée dans plusieurs interventions au cours de la décennie 1990, a laissé une large part aux rapports avec les humanitaires, et aussi aux réseaux sur le terrain. Des pays comme les USA pratiquent les ACM de manière plus institutionnelle. La dimension "formatage", pour ne pas dire idéologico-politique, n'est pas négligée, comme le montrent des institutions comme le *Center for Civil-Military Relations,* qui forme de nombreux étrangers.

La quête du *soft power*. Cette expression, lancée par le doyen Joseph S. Nye (1998), gagne le statut de concept clé des relations internationales. Si l'Amérique prédomine dans le domaine du *"hard power"*, en particulier militaire, dit en substance Nye, elle doit aussi son statut d'hyperpuissance à sa capacité de séduire et d'attirer. L'appel à rétablir un *soft power* submergé par l'antiaméricanisme et décrédibilisé par une guerre contre-productive devient une des constantes du discours critique contre G. W. Bush.

Les rivalités d'influence. Le *soft power* n'est pas un monopole américain. La montée de l'Inde et de la Chine s'accompagne d'une amélioration de leur image. Et il n'y a pas besoin d'être expert en géopolitique pour comprendre que les jeux olympiques de Pékin sont une gigantesque opération d'influence, exactement comme l'offensive de séduction en direction de l'Afrique.

Notre pays a été lui-même un des premiers à lancer une politique d'influence : qu'était-ce d'autre que les Alliances Françaises créées après la défaite de 1870, sinon un moyen de la rétablir auprès des élites étrangères ?

Nous vivons des temps de démocratie d'opinion, d'explosion des médias, de montée en puissance de l'expertise, des "autorités morales" des ONG et autres représentants de la société civile, d'internationalisation des courants d'opinion, d'appels perpétuels à la gouvernance et au consensus…, autant de facteurs qui accroissent le rôle de l'influence. Encore faut-il comprendre que celle-ci ne peut se résumer à une liste de recettes : elle suppose une stratégie globale à la fois économique, politique et culturelle. L'accepter serait déjà un grand pas.

**** François-Bernard Huygue,*** *expert associé à l'IRIS, consultant et écrivain, enseigne en médiologie & intelligence stratégique. Dernier livre sur ce thème :* Comprendre le pouvoir stratégique des médias *(Éditions Eyrolles, 2005).*

Les logiques de sécurité nationale ou les différents moyens de la puissance

*Alain Belleface et Éric Delbecque**

Force est de constater qu'aux États-Unis, la notion de sécurité nationale recouvre en fait la désignation d'une authentique politique de puissance et pas simplement la poursuite d'un projet défensif. Le cas de la sécurité économique démontre de manière emblématique ce processus d'intégration d'une volonté d'accroissement de puissance sous le vocable sécuritaire.

Peu après son arrivée à la tête de la Maison Blanche, Bill Clinton déclara en effet que *la CIA devait se focaliser davantage sur les intérêts économiques des États-Unis*. Il créa alors l'*Advocacy Center* au sein du département du Commerce. Cette structure avait pour objet de favoriser les exportations américaines en aidant la plupart des entreprises nationales (grandes, moyennes et petites) à conquérir des parts de marché à l'étranger. L'*Advocacy Center*, sorte de guichet unique d'entrée et de sortie voué au développement économique du pays, se voyait doté de moyens d'actions bien réels, afin d'aider de différentes manières l'ensemble des acteurs économiques américains. On comptait, par exemple, au nombre de ses missions la possibilité de rédiger des courriers à un gouvernement étranger, de contacter un fonctionnaire étranger de haut niveau, de convoquer une réunion avec un ambassadeur en poste aux États-Unis, ou encore de s'adresser à un cabinet ou une mission commerciale d'un pays étranger.

Une logique d'investissements directs *via* des sociétés écrans, mais pilotée par les pouvoirs publics, fut également mise en place. Ce principe repose sur la prise de participations, par des sociétés sous contrôle des services de renseignement américains, dans le capital de sociétés innovantes (dans des technologies ayant des applications jugées stratégiques en terme de sécurité). L'intérêt de cette action est multiple, car elle permet de :

- réduire les coûts de développement interne de certaines applications nécessaires aux agences de renseignement ;
- promouvoir la recherche et le développement de sociétés ayant un savoir-faire particulier sur des niches technologiques afin de les utiliser au plus tôt au profit de la sécurité nationale ;
- sanctuariser des sociétés ayant développé un savoir-faire qui a des applications à forte connotation sécuritaire afin de prévenir tout risque de mainmise par une puissance étrangère ;
- participer au développement des sociétés américaines de haute technologie, en faisant en sorte que ces sociétés deviennent fortement concurrentielles, voire leaders dans leur domaine.

Les cas In-Q-Tel, ACCIC et OnPoint Technologies.

In-Q-Tel est l'illustration emblématique de ce modèle. Cette société de capital-risque a été créée au cœur de la Silicon Valley par la CIA en 1999. Sa mission est en premier lieu de détecter des technologies innovantes susceptibles d'être utilisées par l'agence de renseignement dans le cadre de ses missions d'espionnage, puis de financer les sociétés les plus avancées ou les plus prometteuses dans les secteurs sélectionnés, selon le principe classique de l'incubation des *start-ups*. Les sociétés dans lesquelles In-Q-Tel a investi sont pour la majorité particulièrement innovantes et essentiellement spécialisées dans la conception de logiciels et de moteurs dédiés à l'analyse linguistique, la récupération de données sur les réseaux informatiques ou encore la sécurité.

Sur le même modèle qu'In-Q-Tel, la NSA a créé sa société de capital-risque en juin 2003. L'ACCIC *(Arundel Country Chesapeak Innovation Center)* est ainsi chargé d'entrer dans le capital des sociétés dont les développements ont une application directe pour la sécurité nationale et la lutte anti-terroriste. L'ACCIC accueillait déjà dans son portefeuille en décembre 2003 sept sociétés dont *Secure Processing*, spécialisée dans les technologies de chiffrement.

Avec OnPoint Technologies, le Pentagone s'est également doté de capacités de financement de sociétés innovantes afin d'accélérer la recherche dans le domaine des technologies susceptibles d'être utilisées par les forces armées. L'US Army a ainsi confié 25 millions de dollars à la société OnPoint Technologies en mai 2003 pour détecter des *start-ups* prometteuses. L'un des axes prioritaires se trouve être les technologies liées à la fabrication de sources d'énergies miniatures de nouvelle génération telles que les micropiles à combustibles.

La stratégie états-unienne de projection commerciale.

Le gouvernement américain a également mis en place une stratégie de participation à l'équipement des infrastructures à l'étranger. En matière d'équipements et d'infrastructures des télécoms, les États-Unis ont une politique très affirmée et particulièrement offensive, notamment dans les pays en voie de développement (Afrique en particulier) et dans les zones de conflits (Afghanistan, Irak ou ex-Yougoslavie). La méthode consiste, soit à offrir littéralement le matériel et les infrastructures, soit à sanctuariser les nouveaux marchés émergeants par le biais d'appels d'offres destinés quasi-exclusivement aux entreprises américaines.

La force des États-Unis en la matière est qu'ils disposent de moyens financiers sans commune mesure par rapport aux autres pays qui tentent de mener la même démarche, notamment auprès d'anciennes colonies. Là où la France, par exemple, qui participe à l'équipement de certains pays africains, expédie en général du matériel de l'administration, ancien et "réformé", les États-Unis n'hésitent pas à donner du matériel neuf et technologiquement actuel. S'ajoute à cela la formation des personnels qui seront amenés à s'en servir et surtout un service après vente et de

maintenance très performant allant jusqu'au détachement permanent de techniciens américains au sein des administrations ou des opérateurs télécoms nouvellement équipés.

Le passage du secteur public au secteur privé (et inversement) fait partie de la culture des États-Unis. La passerelle entre activités sensibles et commerciales y est monnaie courante. De fait, à tous les niveaux du monde des affaires, un réseau étendu de collaborateurs est en mesure d'influencer une prise de décision, d'obtenir des renseignements précis sur des sujets particuliers, constituant autant d'honorables correspondants au service de l'État.

Il faut encore évoquer l'acquisition de technologies étrangères et la sanctuarisation des technologies nationales. Parmi les différents outils dont disposent les États-Unis pour asseoir leur suprématie dans le domaine des technologies d'information et de communication, les *fonds de pension* représentent un moyen très efficace permettant l'acquisition de technologies innovantes développées à l'étranger.

Les États-Unis se servent en effet de l'argent comme d'une arme à part entière. En utilisant habilement les règles du commerce international et de la libre concurrence, permettant les investissements à l'étranger, et les législations des différents États dans le domaine, les États-Unis arrivent à développer leur stratégie de puissance en tout légalité.

En outre, les États-Unis cultivent avec habileté l'art du lobbying et de l'influence tant sur le territoire américain qu'à l'étranger, en particulier auprès d'instances internationales (ONU, UIT, etc.), au travers de toute une série de structures aux statuts les plus divers, comme les cabinets de conseil et de relations publiques, les associations ou encore les *Think Tanks*. Chacune de ces entités, à des degrés différents, participe à l'accroissement de la puissance américaine dans le domaine de la défense notamment, et en particulier dans le domaine des technologie d'information et de communication. Particularité américaine : les *Think Tanks* participent activement à influer sur les prises de décision de l'administration américaine, tant dans le domaine politique que commercial. Ils peuvent également, par les conclusions de leurs travaux, justifier des décisions politico-stratégiques déjà prises, ou à venir, par les autorités américaines.

La sécurité nationale en Chine. "En fait, expliquent deux officiers chinois, Qiao Lian et Wang Xiangsui, dans un texte intitulé *La guerre hors limites*, non seulement les États-Unis, mais tous les pays qui ont le culte de leur puissance ont déjà inconsciemment élargi les frontières de la sécurité à de nombreux domaines comme la politique, les ressources naturelles, les minorités, la religion, la culture, les réseaux, la géographie, l'environnement et l'espace. Cette vision *pan-domaines* est une des conditions de la survie et du développement des États souverains modernes ainsi que de leur influence dans le monde. En comparaison, la vision de la défense nationale comme principal objectif de la sécurité apparaît assez dépassé, à la rigueur très incomplète."

L'émergence décisive du géant chinois sur la scène internationale témoigne d'un clair projet de puissance qui rappelle les thèses des deux auteurs de *La Guerre hors limites*. Pour le gouvernement de Pékin, cette situation apparaît comme la restauration d'un ancien statut, perdu au début du XIX^{e} siècle. Mais il est aujourd'hui difficile de trancher clairement : faut-il donner crédit aux proclamations appelant à l'édification d'un monde multipolaire, ou pister tous les indices d'une aspiration à l'hégémonie ?

En tout état de cause, la Chine veut affirmer son leadership asiatique au travers d'un déploiement stratégique au sein des institutions internationales. Son adhésion à l'Organisation mondiale du commerce (OMC) en 2001 lui a d'ailleurs permis de franchir une étape décisive.

La Chine édifie également une stratégie d'influence en Afrique, en particulier dans les pays pétroliers. Elle vise ainsi à sécuriser ses approvisionnements en énergie et matières premières. En outre, l'implantation chinoise en Afrique dépasse très largement les relations commerciales : Pékin multiplie les échanges universitaires, installe des centres commerciaux chinois et investit le domaine des travaux publics. Pékin développe également ses relations avec l'Amérique du Sud. En fait, il apparaît clairement que la Chine investit fortement dans les zones relativement délaissées par les pays occidentaux. Cette stratégie d'expansion met en lumière des enjeux non seulement commerciaux mais également politiques, lesquels s'inscrivent clairement dans une stratégie de puissance dont il est encore difficile de mesurer les intentions réelles et les conséquences de moyen et long terme.

Un enseignement pour la France. Après ces brèves réflexions sur la sécurité nationale aux États-Unis et en Chine, l'enseignement que peut en tirer la France paraît évident. Ces deux pays se caractérisent par l'existence de véritables stratégies de puissance nationale portées par un discours de sécurité nationale. L'absence, ces dernières années, d'un projet de puissance explique à la fois le retard d'élaboration d'une authentique stratégie de sécurité nationale en France et l'inexistence d'une stratégie de sécurité européenne globale (l'Union n'ayant pas réussi à définir des objectifs stratégiques communs susceptibles d'alimenter un projet communautaire d'influence au niveau mondial). ■

* ***Alain Belleface*** *est directeur associé de la société LMCI. Il a travaillé durant plusieurs années à la DGSE, où il a notamment été en charge des dossiers relatifs aux technologies de l'information. En 2007, il fut pendant un an le responsable du pôle sécurité de l'information du cabinet Risk & Co.*

Éric Delbecque, *secrétaire général de l'IERSE (Institut d'Études et de Recherche pour la Sécurité des Entreprises), est notamment l'auteur de* Quel patriotisme économique ? *(PUF, 2008).*