

RECONSTRUIRE LA PENSÉE STRATÉGIQUE

NOUVELLES MENACES ET SÉCURITÉ NATIONALE

En quelques semaines, tout ce qui avait été oublié, ou occulté, est revenu au premier plan de l'actualité. Citons : l'instabilité financière, dénoncée pour ce qui était des normes comptables ou de la création de produits dérivés de dérivés, il y a près de dix ans par Claude Bébéar ou nous-mêmes dans une remarquable indifférence ; la guerre en Afghanistan avec des pertes françaises importantes lors d'un seul accrochage, sur un terrain connu de tous comme l'un des plus dangereux au Monde (le géopoliticien Mahan suggérait d'éviter le pays en passant par les mers) ; le conflit en Géorgie, aux portes de l'Union européenne, marqué par une absence de réaction historique des Etats-Unis... La surprise stratégique, qui surprend en général ceux qui ne veulent pas voir, est de retour. Depuis le début des années 90, sous l'impulsion notamment de Xavier Raufer, un groupe informel a décidé, à l'occasion de notes d'alerte régulières, puis de la publication d'un "Etat des menaces" trimestriel, de déceler les mutations à venir, de détecter les signaux faibles, de mettre en place un outil et une méthodologie adaptés aux conflits criminels, terroristes comme aux évolutions stratégiques. Régulièrement, TTU tentera de s'en faire l'écho.

Alain Bauer et Xavier Raufer, criminologues

Pourquoi passer de la "défense globale" à la "sécurité globale" ?

Il devient urgent de combler le vide de la pensée stratégique.

Pendant longtemps, on a cru, ou feint de croire, que la France disposait depuis toujours d'une stratégie de sécurité nationale claire, établie, stable, défiant le temps et les menaces.

Après une longue période de doute et de gestion des aigreurs de la défaite de 1940, puis des effets conjugués des opérations militaires liées à la décolonisation (dont certaines furent des réussites militaires mais autant d'échecs politiques ou diplomatiques), la reconstruction de l'outil militaire national autour de la stratégie de dissuasion nucléaire, voulue par le Général de Gaulle dès la Libération puis par tous ses successeurs, permit une résurrection conceptuelle autant que matérielle de la stratégie de défense nationale. Les problématiques de sécurité intérieure et de lutte contre le terrorisme n'en furent pas exclues du fait de la situation indochinoise (sur place) ou algérienne contre le FLN s'appuyant sur la Willaya de France continentale puis contre l'OAS. Les travaux du colonel Trinquier servirent même de

produit à l'export, enseignés dans la tristement célèbre Ecole des Amériques.

Il faut rappeler l'exceptionnelle qualité de l'encadrement policier ou militaire français. Et la toute aussi exceptionnelle crise de la pensée sur les sujets stratégiques majeurs. Certes, les grands anciens étaient assez atypiques et peu soutenus. Mais il existait une richesse de production intellectuelle que des efforts récents, au Centre de doctrine de l'armée de terre, dans les revues Inflexions ou Champs de Mars, ne sont toujours pas parvenus à retrouver.

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.

Dans son dernier ouvrage, «La guerre probable», le plus intéressant travail mené récemment, le Général Desportes le rappelait.

Voici pourquoi la reconstruction d'une pensée stratégique est un passage obligatoire. Voici pourquoi la sécurité globale doit intégrer défense nationale, sécurité publique, sécurité des entreprises, sécurité environnementale et s'appuyer sur un outil souple de décèlement précoce. Car, depuis la fin de la Guerre froide, terrorisme et crime organisé ont connu une mondialisation qui déborde du cadre étatique, statique et rétrospectif où ils s'étudiaient hier.

Le plus souvent, en matière criminelle ou terroriste, ce qui est nouveau, c'est ce qu'on a oublié. En matière criminelle, Conan Doyle fait dire à Sherlock Holmes que ce qui reste, une fois l'impossible supprimé, même si c'est incroyable, doit être la vérité. Or, avant le 11-Septembre, en matière de terrorisme, ce qui était incroyable était supposé impossible.... Par inertie, par faiblesse ou par peur de la réaction des supérieurs, les forces de police et de renseignement n'ont pu accepter de traiter de l'incroyable. Et l'incroyable est devenu réalité.

GLOBALISATION CRIMINELLE ET ÉCOTERRORISME

L'EUROPE DU CRIME

Depuis la chute du mur de Berlin, 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, avec leurs zones de chalandises, leurs promotions des ventes, leurs études de marché, leur gestion, plutôt définitive, de la concurrence, leurs politiques d'investissements, leurs cadres, leur management....

L'Europe du crime est déjà faite, Turquie incluse, avec sa maffiyah spécialisée dans le service aux autres groupes criminels. L'Europe de la Police et de la Justice reste à faire. Le Monde du crime est déjà globalisé, seule sa police reste morcelée. Et il se développe par le blanchiment et par le contrôle des territoires de la drogue, de la prostitution, des trafics. La mondialisation des implantations financières off-shore est une réalité physique.

De l'optimisation fiscale (le joli nom pour évasion) au blanchiment, en passant par le racket, la corruption et la rétro commission, les mêmes tuyaux servent à tout. Seuls les branchements diffèrent. Les triades chinoises se sont parfaitement accommodées du régime politique, les organisations criminelles indiennes prospèrent à Bombay et ailleurs, les espaces tranquilles ne sont pas toujours sûrs.

POUR UN MANAGEMENT DE L'ÉCOTERRORISME

En mars 2008, cinq engins explosifs déclenchent des incendies

qui ravagent un quartier résidentiel en construction à Seattle, plusieurs millions de dollars de dégâts (action revendiquée par l'ELF, le Front de Libération de la Terre). En décembre 2007, le domicile d'un fourreur de Bordeaux est tagué, ses numéros de téléphone publiés sur Internet et la porte de son garage incendiée par l'ALF (Front de Libération des Animaux). Ces deux actions illustrent les méthodes des mouvements extrémistes de la cause animale. Nés dans les années 70 dans les pays anglo-saxons, ces mouvements – notamment l'ALF – se réclament de l'antispécisme, une doctrine prônant l'absence de différence entre les espèces et l'égalité entre les «animaux humains» et «non-humains». Revendiquant une filiation avec les combats de l'antiracisme et du féminisme, ce mouvement s'est peu à peu diffusé, notamment dans les pays latins. Les mouvements antispécistes utilisent tout moyen pour rendre les activités des «exterminateurs d'animaux» (volontiers comparés aux nazis) le moins économiquement rentables possible.

«Cibia vision et Novartis doivent ressentir la douleur des animaux qu'ils tuent.» C'est à partir de ce communiqué publié sur le site Bite

Back, en août 2007, que l'ARM (Milice des Droits des Animaux, considérée comme plus radicale que l'ALF) annonce avoir empoisonné 85 bouteilles de solutions pour lentilles ophtalmologiques produites par Novartis, entreprise pharmaceutique coupable, à ses yeux, d'être cliente d'HLS (Huntingdon Life Sciences, l'une des principales entreprises d'expérimentation animale). Il en résulte le retrait de dizaines de milliers de flacons de ces solutions, en France comme en Grande-Bretagne. Le préjudice est conséquent, tant financièrement qu'en terme d'image, pourtant aucune contamination n'est constatée.

L'attaque est informationnelle ; l'arme est économique. Dans le secteur mondialisé et concurrentiel actuel, les dommages provoqués par la désinformation du consommateur peuvent s'avérer redoutables. Le mode opératoire a déjà fait ses preuves outre-Atlantique ainsi qu'en Italie, où l'annonce, en 1998, par l'ALF local de l'empoisonnement de gâteaux de Noël a conduit le fabricant, filiale du groupe Nestlé, à retirer ses produits de la vente. L'objectif est l'atteinte à l'entreprise : nuire à la réputation et frapper financièrement, tels sont les deux aspects de l'«ecotage», sabotage économique.

La progressivité de l'engagement des cellules opérationnelles conduit à une montée en puissance de l'intensité des actions menées. Des dégradations aux destructions par incendie. Des incendies aux attentats. Les menaces se sont en effet précisées en France, ces deux dernières années. Tant par l'intensité des actes que par les cibles désormais choisies : des acteurs directs de la chaîne de la recherche scientifique.

Des modes opératoires différents privilégient l'envoi par la Poste de lames de rasoir ou de colis piégés. En France, en 1985 déjà, l'explosion d'un colis reçu par un éleveur d'animaux de laboratoire dans la Sarthe avait blessé un gendarme.

Cette violence radicale n'est toutefois portée en France, à l'heure actuelle, que par un nombre restreint d'activistes radicaux, proches des milieux anticapitalistes. La réponse implique pour chacun une véritable politique de management du risque écoterroriste.

Julien DUFOUR, commissaire de la Police Nationale, criminologue au Département de Recherche sur les Menaces Criminelles Contemporaines.

Stéphane QUERE, criminologue au Département de Recherche sur les Menaces Criminelles Contemporaines

LES MENACES CONCURRENTIELLES

A la fin des années 90, deux colonels de l'armée chinoise, Qiao Liang et Wang Xiangsui, ont rappelé dans un livre stimulant, intitulé "La Guerre hors limites", que les espaces de conflits n'ont pas disparu mais se sont métamorphosés et sans doute élargis. S'évadant des champs de bataille, la guerre a investi le cyberspace, le commerce mondial, la finance internationale, l'échiquier médiatique...

Dès lors, chaque acteur économique devient un loup pour tous les autres acteurs économiques... Aucune paraphrase ironique de Hobbes dans ce propos mais simplement une évidence facile à constater : dans les différents épisodes de l'affrontement Boeing/EADS, pour prendre ce seul exemple, l'hyperconcurrence se laisse aisément contempler dans ses multiples dimensions...

Un défi pour les entreprises

L'entreprise fait clairement face aujourd'hui à des menaces concurrentielles. Dans l'ordre des manœuvres illicites (auxquelles certaines entreprises, malheureusement, n'hésitent pas à recourir), on citera le vol ou l'interception de données, l'atteinte à l'image par la désinformation, l'intrusion dans la vie privée de dirigeants ou de salariés occupant des postes clefs, le sabotage de systèmes d'informations...

Bien évidemment, les profits de l'entreprise pâtissent les premiers des offensives concurrentielles. Mais l'emploi ne tarde pas à en subir également les conséquences. Et c'est aux entreprises que revient la tâche prioritaire d'adapter leur culture, laquelle n'est pas spontanément portée à anticiper ces menaces concurrentielles. Toutes les études le confirment, écrivait avec raison Christophe Babinet : «Lorsque les entreprises daignent se préoccuper de sécurité, c'est très généralement en envisageant le seul aspect de la protection physique de leurs locaux ou des équipements qui s'y trouvent.

Beaucoup plus rarement de ce bien impalpable et volatil : l'information. Et plus rarement encore en sensibilisant leurs salariés aux artifices utilisés par les capteurs d'informations.»

Pour répondre aux différentes menaces concurrentielles qui peuvent l'affecter, l'entreprise doit d'abord mettre en œuvre un solide dispositif de veille pour anticiper une partie d'entre elles (notamment la préparation d'offensives informationnelles). Dans un deuxième temps, l'entreprise doit assurer la protection de l'information stratégique, celle-là même qui lui permet de garantir son avantage concurrentiel. Il est indispensable de rénover radicalement notre perception et notre conception de la sûreté. Elle permet de créer de la richesse et de valoriser des compétences.

La réponse adéquate

Ce qui fait la valeur ultime d'une entreprise doit demeurer inconnu pour ses concurrents avérés ou potentiels. Le risque est ainsi le pendant exact de l'opportunité. S'il ne faut pas se «bunkeriser», il est en revanche urgent de perdre toute naïveté face aux conséquences de l'hyperconcurrence mondiale.

Les modalités opérationnelles ou le périmètre de sécurisation de l'information dite sensible peuvent légitimement prêter à discussion. A tout instant, il faut en effet s'interroger sur la pertinence du secret. Que faut-il protéger et que doit-on laisser circuler comme type d'informations, de données et de connaissances ? Seule la concertation entre les experts au sein même de l'entreprise, entre les différents acteurs de la création de valeur (par exemple les groupes, les PME-PMI et les centres de recherche et les universités sur un pôle de compétitivité), entre l'Etat et les sociétés dans le domaine des technologies de souveraineté, permet au cas par cas d'arbitrer en faveur de la rétention de l'information ou de sa diffusion plus ou moins large et réglementée. Le transfert de

technologies illustre de manière emblématique cette problématique. Mais c'est le changement de culture qui devient urgent.

En matière de guerre de l'information, la désinformation est la production d'informations fausses, c'est-à-dire relatant des faits n'ayant pas existé. Mais cette définition doit être élargie, comme le précisait récemment et pertinemment Jacques Myard, «au cas où désinformation signifie production d'informations déformant la réalité de faits avérés». La désinformation caractérise aujourd'hui quelque chose de différent du simple mensonge : elle désigne une manière délibérément biaisée de présenter une information.

Avoir une stratégie d'influence

Les entreprises ne peuvent pas non plus faire l'économie de l'élaboration et de la mise en œuvre de véritables stratégies d'influence visant à renforcer leur sécurité. C'est un travail de soft power. Cette démarche d'influence dépasse le cadre du simple lobbying et exige une véritable stratégie.

Dans les deux domaines, normes juridiquement contraignantes ou Soft law, il s'agit en fait de mettre en œuvre des stratégies d'influence adossées, en amont, à une production conceptuelle à vocation pratique.

Pour conclure, il importe donc de mettre en avant une typologie des menaces concurrentielles majeures et relativement nouvelles auxquelles les entreprises doivent répondre. Captation d'informations stratégiques, attaques sur les systèmes d'information, guerre par l'information (c'est-à-dire l'utilisation des médias comme instruments de déstabilisation), et affaiblissement par encerclement normatif, apparaissent comme les quatre grandes formes de menaces concurrentielles dont les entreprises peuvent être les victimes.

Eric Delbecque,
directeur de l'IERSE

CYBERCONFLITS : UN DÉFI POUR LES ARMÉES

Au cœur de toutes les préoccupations actuelles, l'arme digitale fascine. Depuis les événements d'avril 2007 en Estonie, l'éventualité d'un cyberconflit est présente dans tous les esprits. Le premier point concerne différents types d'armes et d'attaques digitales :

- Les attaques destructives niveau 2 de type Ddos (saturation des serveurs par de fausses requêtes) qui entraînent une paralysie des réseaux (exemple de l'Estonie), menées par des Botnets (réunion de PC pour construire une armée de soldats numériques), comme Storm Worm, auxquels aucune infrastructure ne pourrait résister à ce jour.

- Celles ayant pour objectif la récupération d'information sensible sur des serveurs d'entreprises ou de l'Etat (militaires ou administratifs). Exemple de la Chine.

- Celles non avérées mais réalisables et pouvant engendrer des incapacités majeures (attaque des systèmes SCADA sur des infrastructures stratégiques : nucléaire, électricité, traitement de l'eau, etc.).

- Les attaques destructives niveau 1 (défaçage de site Web, attaques de Ddos, envoi de Trojan ou autre code malveillant, vol, destruction ou modification de données, etc.).

- Les attaques physiques liées aux infrastructures informatiques, coupure de câbles, vol ou destruction de machines.

- Moyens de pression sur le personnel civil ou militaire, corruption et menaces.

Le deuxième point se situe au niveau de la qualification des armes numériques. Les systèmes d'information d'une centrale électrique ou nucléaire

sont aussi vulnérables et, selon une étude récente du DHS (Department of Homeland Security) aux Etats-Unis, les générateurs électriques peuvent être piratés et s'autodétruire par des commandes transmises à distance relevant ainsi la menace à un niveau de risque de destruction massive.

Le troisième point porte sur les ressources humaines nécessaires au déploiement de ces armes. Car l'étincelle qui anime les génies du clavier ne s'acquière pas sur les bancs de l'université, elle touche indifféremment un individu quelles que soient ses origines sociales et culturelles.

Pour mener une attaque destinée à récupérer de l'information située sur des réseaux informatiques étrangers, il faut développer un cheval de Troie furtif et crypté, indétectable par les systèmes de protection les plus sophistiqués. Pour cela il doit être envoyé à la cible en exploitant une vulnérabilité applicative ou système encore jamais découverte (Zero Day Attaque) et pour laquelle il n'existe donc pas encore de protection.

Il y a un marché mondial des vulnérabilités avec des cotations en fonction de la faille découverte. La valeur de ces découvertes varie selon les acheteurs et surtout selon leur degré de légalité, les entreprises de sécurité ou les départements de sécurité d'éditeurs de logiciels ou de systèmes d'exploitation achèteront des failles entre 500 et 30 000 dollars, les prix peuvent atteindre 250 000 dollars dans les organisations criminelles.

Le quatrième point concerne l'identification des auteurs d'une attaque. Les techniques de rebond employées

par les Botnets et pire encore ceux utilisant le fast-flux DNS sont impossibles à retracer. Le problème qui se pose alors est d'arriver à définir si une attaque est menée par une unité spéciale appartenant à un Etat, si elle est l'œuvre d'un groupe de pirates agissant pour le compte d'un gouvernement ou si elle vient d'hacktivistes motivés par des convictions politiques.

Enfin le cinquième point porte sur la capacité de réponse compte tenu des éléments précédemment évoqués. Se défendre est une priorité, répondre est une nécessité, mais à qui et dans quelle mesure ? L'Estonie avait accusé le gouvernement russe d'être impliqué dans les attaques Ddos qu'elle avait subies, ce dernier avait immédiatement démenti. Aujourd'hui, grâce à l'Otan, l'Estonie est équipée d'un centre de cyberdéfense réalisé et financé conjointement par l'Allemagne, l'Italie, la Lituanie, la Slovaquie et l'Espagne. Si ce centre avait été opérationnel en avril 2007, les autorités estoniennes, alors convaincues de l'implication du gouvernement russe, l'auraient peut-être utilisé à tort pour riposter. Si l'Estonie avait répliqué en attaquant la Fédération de Russie, celle-ci aurait pu, à juste titre, considérer cela comme un acte de guerre.

Ces réflexions mènent à la conclusion que si la création d'un cybercentre de défense doté d'armes numériques offensives est indispensable, le déclenchement de son utilisation reste encore à définir en raison de l'incapacité pour les Etats de gérer les groupes autonomes capables de lancer des attaques sans aucun contrôle possible des autorités.

Laurence Ifrah, criminologue au Département de Recherche sur les Menaces Criminelles Contemporaines

CE NUMÉRO SPÉCIAL EST PUBLIÉ AVEC LE SOUTIEN D'AB ASSOCIATES, CONSEIL EN SÉCURITÉ GLOBALE.