Les nouvelles technologies au service de la prévention et de la protection contre le terrorisme : état des lieux technique
août 2006

Les technologies contre le terrorisme : anticiper, choisir, investir

S'il faut garder à l'esprit que le « tout » technologique est inefficace pour enrayer le terrorisme – phénomène à la fois social, politique et religieux dans le cas d'Al-Qaïda – il est en revanche nécessaire de prendre la mesure du vaste panel de réponses que les technologies nous offrent pour se prémunir des effets du terrorisme. Face à une menace globale, inattendue, dont on ne connaît ni la forme ni l'ampleur, trois orientations en matière de défense nationale devraient être adoptées : 1. La première priorité devrait être celle d'investir dans des technologies capables d'intégrer toutes les technologies existantes dans un système global cohérent et efficace ; une technologie des technologies en somme (partage des compétences et des connaissances, synergie des actions, échanges numériques sécurisés, réseaux dédiés, bases de données intégrées). 2. Par ailleurs, face à une menace durable, il faut développer des technologies à la fois efficaces et rentables car mieux vaut économiser et cibler les investissements sur des technologies flexibles plutôt que d'investir peu dans tous les domaines. 3. Enfin, il faut favoriser les technologies de pointe. Les groupes terroristes, même s'ils ne disposent que de moyens et de ressources limités, cherchent en permanence de nouvelles techniques pour frapper au cœur de nos sociétés. Briser le cercle de l'innovation entre les terroristes et les forces anti-terroristes nécessite un bond technologique de grande ampleur, afin qu'ils ne puissent rattraper leur retard. Cet effort d'innovation ne doit pas à l'inverse « faire écran » devant nos faiblesses dans des secteurs technologiques plus traditionnels. Plutôt que d'adapter a posteriori les technologies aux dangers avérés, il faut anticiper ceux-ci et développer des systèmes au champ de protection le plus large possible. La Révolution dans les Affaires Militaires (RMA), initiée aux États-Unis, peut y contribuer en adaptant les technologies traditionnelles à la nouvelle donne terroriste.

Les drones : surveiller et punir à distance

La RMA, mutation technique (numérique) des forces militaires conduisant à une refonte générale de leur doctrine d'emploi (ubiquité) et à des évolutions organisationnelles, n'est pas la réponse définitive au terrorisme. En effet, l'antagonisme qui oppose les puissances démocratiques occidentales aux réseaux terroristes informels se caractérise par son asymétrie, c'est-à-dire par l'écart des moyens technologiques à la disposition de chacun des deux camps. Mais l'application de la RMA pourrait s'avérer être un moyen de transformer cette asymétrie en avantage décisif pour les occidentaux et faire face à la multiplicité des menaces terroristes. Avec la RMA, la veille permanente est plus efficace. La révolution de l'informatique et des réseaux a trouvé une application remarquable pour cette tâche : les drones aériens ou UAV (*Unmanned Air Vehicle*). Application d'autant plus intéressante qu'elle agrège sur un engin conventionnel la RMA au concept du « zéro mort », puisque ce sont des aéronefs miniaturisés et sans pilote, capables de réaliser une vidéosurveillance en temps réel, d'emporter des charges et de l'armement (attaque à distance). Un « système de drone » est composé d'un vecteur et d'une ou plusieurs stations de commande. Les drones peuvent être aériens, terrestres ou marins et on en distingue quatre grandes familles : les mini (classe de coût 4500 euros), les tactiques (1,5 millions d'euros), les MALE (Moyenne Altitude Longue Endurance) opératifs (10 millions d'euros), et les HALE (Haute Altitude Longue Endurance) stratégiques (100 millions d'euros). L'armée de terre française s'est dotée de Systèmes de Drones Tactiques Intégrés (SDTI). L'armée de l'air disposera d'ici 2008 de drones tactiques MALE. La France accuse un certain retard par rapport aux États-Unis et Israël qui utilisent des drones non seulement sur les champs de batailles mais aussi pour surveiller leurs frontières. Les premiers surveillent l'infiltration de clandestins à la frontière mexicaine, les seconds identifient et ciblent « au-delà de la colline » les groupes terroristes palestiniens préparant des attaques au mortier au-dessus de la frontière. *Israël Aircraft Industries*, en pointe dans ce domaine, a vendu en 1998 à la France le système de drone aérien *Hunter* et a développé

pour la première fois en 2003 une classe de micro-drones (250 g., 30 cm d'envergure, 40 min. d'autonomie).

***Datamining*, armes à énergie dirigée, biométrie et nanotechnologies : outils de sécurisation**

Le *datamining* (forage de données) contribue à la mise en place d'une « technologie des technologies ». Il permet de créer des bases de données, d'en extraire automatiquement des informations précises et référencées et, par corrélation des occurrences, de classer l'information selon certains critères. Des données sans liens apparents sont mises en relation. La masse d'informations ainsi réorganisée permet une prise de décision et des prévisions plus rapides, plus rationnelles. Dans le domaine militaire, les applications sont nombreuses : modélisation de phénomènes physiques complexes, classification de signaux (discrimination des cibles), reconnaissance de formes (identification des cibles), sécurisation des systèmes d'information, renseignement (pour intercepter et analyser des communications de terroristes par exemple), soutien à la logistique. Le système *Echelon* d'interception des communications privées et publiques témoigne de l'intérêt que portent les États-Unis à cette technologie. Les armes à énergie dirigée (lasers, radiations micro-ondes) atteignent leur cible à la vitesse de la lumière et les soumettent à une énergie concentrée (sans perte). Des lasers pourraient être installés dans les aéroports, voire sur les avions eux-mêmes, pour parer toute attaque par roquette, missiles. *Northrup Grumman* et *Lockheed Martin* ont déjà équipé de quatre lasers et de six censeurs anti-missiles un Boeing 747 (programme ABL).

La biométrie, qui a déjà trouvé de nombreuses applications dans la vie quotidienne (passeports biométriques, accès à des locaux par reconnaissance faciale, vocale, des veines, par l'iris de l'œil, par empreintes digitales), propose un large éventail de solutions pour sécuriser notre espace en interdisant la libre circulation aux personnes non-autorisées. Ces applications, qui ne sont pas toutes fiables ni pratiques, sont comme toute technologie sujettes aux pannes et au piratage. La biométrie la plus avancée porte sur la reconnaissance cérébrale. La société américaine *Brain Fingerprint Laboratories*, créée en 2003, serait capable de détecter si le cerveau d'un individu a « enregistré » la spécificité d'un entraînement pour des activités terroristes (détection d'une mémoire fonctionnelle). Les nanotechnologies n'en sont qu'au stade de la recherche fondamentale mais les potentialités semblent considérables. Les nanostructures électroniques permettront de réduire la taille des composants à l'échelle atomique et par là, augmenteront les performances des ordinateurs. Les nanostructures biomédicales (échelle moléculaire) permettront de cibler l'usage d'un médicament, de créer des éléments adhésifs pour fixer des greffes de peau. Les nanotechnologies permettront la méta-convergence des technologies de l'information et de la communication, des biotechnologies, des sciences et technologies cognitives. Investir dans les nanotechnologies doit être une priorité.