Terrorisme du XXIéme siècle

(Guide pratique du terrorisme)

Par
Atta Oloumi

Association Atta Oloumi

Terrorisme du XXIéme siècle

(Guide pratique du terrorisme)

Par
Atta Oloumi

Association Atta Oloumi

SOMMAIRE

PRÉFACE

Ce livre inachevé est une lanterne translucide qui nous éclaire les chemins parcourus, mais le terrorisme de la route ne lui a pas accordé le temps de nous éclairer le reste des chemins inconnus.

Atta Oloumi a été tué dans un accident de voiture le 26 novembre 1999 sur l'autoroute de Rouen par une meurtrière en liberté et impunie, par le laxisme de la justice qui traite une affaire de mort avec une légèreté scandaleuse et inhumaine.

Ce qui explique pourquoi la mort est aussi présente sur les routes de France.

Cet événement insondable, encore une fois, met en acte la capacité destructive de l'homme.

Sa mère

(Les recettes de ce livre sont intégralement reversées à différentes associations caritatives pour les handicapés mutilés par les mines antipersonnel.)

BIOGRAPHIE

Atta Oloumi est né le 21 juillet 1965 a Aix en Provence. En 1986 il obtenait une licence de physique, en 1987 une maîtrise de physique fondamentale, et en 1988 un D.E.A. de physique des plasmas.

Le sujet de sa thèse de doctorat est : La stabilisation des systèmes hamiltoniens chaotiques, qui fut publiée en décembre 1999 dans la revue américaine " **PHYSICAL REVIEW E"** (au Etats Unis).

Il était chercheur scientifique au Médical Center of Stanford University sur les applications de la théorie des systèmes dynamiques à la médecine dans deux départements de ce centre: ***F****unctional* ***R****estauration et* ***R****adiation* ***O****ncologiy.*

Journaliste professionnel de 1991 à 1996, il a publié plus d'une centaine d'articles pour des revues scientifiques telle que :

Science & Vie, High Tech , Info P.C., La Recherche , Golden, le Monde Informatique, Industries et Techniques...

Il a écrit un article de fond sur les Supercalculateurs pour la ***Recherche***, ainsi qu'un ouvrage sur "le petit guide des processeurs" publié chez Ellipse en 1994.

Ces derniers temps il développait une nouvelle application des implants Extra-Oraux. Son objective principal était le déplacement des personnes tétraplégiques, surtout les accidentés de la circulation et plus particulièrement les handicapés victimes des mines antipersonnel.

La disparition d'un scientifique talentueux et brillant, qui s'apprêtait a faire avancer l'humanité est incommensurable.

PARTIE 1

IDÉES REÇUES

20 vraies et fausses vérités

L'idée qu'un groupe subversif puisse déstabiliser un gouvernement occidental, voire prendre le pouvoir, est difficile à accepter. Car un grand nombre d'idées reçues donne l'illusion soit d'une sécurité absolue, soit qu'un coup d'État s'accompagnerait d'un cataclysme. Cassons donc pour commencer quelques contre-vérités…

"La puissance militaire des grandes nations interdit toute action d'envergure."

Faux

L'opération des indépendantistes tchétchènes démontre le contraire. En janvier 96, deux cents

combattants se sont emparés de la petite ville de Pervomaïskaïa. Ils n'étaient équipés d'aucune arme lourde (pas de chars, pas de transports blindés ni d'artillerie lourde). Pour libérer la petite bourgade, les Russes ont fait intervenir la division d'actions rapides Sobor du ministre de l'Intérieur, les forces spéciales antiterroristes Alpha, l'armée fédérale et les gardes-frontières. Plusieurs tentatives de reprise de Pervomaïskaïa se sont soldées par des échecs, y compris pour les forces spéciales : toute la ville était minée et des nids de mitrailleuses étaient utilisés par de petites équipes de francs-tireurs. Pervomaïskaïa a donc été rayée de la carte par un déluge d'obus et de roquettes avant que les forces russes puissent y pénétrer. Les survivants du commando tchétchène ont cependant eu le temps de s'enfuir avec des otages, après avoir mené une incursion de plus de deux heures au cœur du dispositif russe sans subir de pertes.

Cet exemple prouve que l'armée est incapable de combattre efficacement des commandos. Elle ne peut intervenir que dans des cas précis où elle a en face d'elle des armes lourdes, visibles et peu mobiles. Or ce concept est aujourd'hui dépassé : un missile peut détruire les chars les plus modernes ; portable, il coûte mille fois moins cher qu'un char. Dans ces conditions, la durée de vie d'un engin blindé se compte en heures, voire en minutes.

C’est toute la leçon des conflits des années 90. D’un côté, l’Irak a déployé des armes et des installations (chars, véhicules de troupes blindés, sites de missiles antiaériens, bunkers, ponts) qui faisaient des cibles parfaites, car visibles. De l’autre, en Bosnie, les armées de fantassins ont combattu à l’aide de pièces d’artillerie tractées faciles à dissimuler dans les montagnes. Dans le premier cas, la victoire militaire occidentale a été totale, dans l’autre il n’a même pas été possible d’intervenir.

“Seule la médiocrité des terroristes nous protège contre eux.”

Vrai

Le terrorisme qui défraie chaque jour la chronique a un relent de XIXe siècle, avec ses bombes rappelant les “machines infernales”. Combien de temps encore les terroristes recourront-ils à des techniques d’un autre âge ? Un État moderne et démocratique peut-il accepter que sa sécurité repose sur la médiocrité de ses adversaires ? Si un vent de violence révolutionnaire souffle de nouveau sur les États occidentaux, il risque fort bien de tout emporter sur son passage. Car même les imbéciles apprennent avec le temps.

Le monde ne sera pas ébranlé par des camions piégés. Tout juste se souviendra-t-on de leurs

victimes innocentes. Les massacres à l'arme chimique de la secte Aum ont fait à peine plus de dégâts que quelques bombes artisanales dans le métro parisien. Les membres de la secte ont bien tenté une action d'envergure en dispersant du haut d'un immeuble de Tokyo une solution liquide contenant les bacilles d'anthrax, mais cette opération s'est soldée par un échec complet, car l'arme bactériologique, tout comme l'arme chimique, est très peu efficace lorsqu'elle est dispersée au gré du vent.

Quand les terroristes utiliseront-ils des missiles, des bombes radioactives, des armes à fragmentation ? Faciles à obtenir, peu onéreuses, de telles armes pourraient faire des dizaines, voire des centaines de milliers de morts. Ces catastrophes nous pendent au nez. Les terroristes ont aujourd'hui les moyens de terrasser les États occidentaux.

"La plupart des programmes militaires sont inutiles."

Vrai

Les lobbies militaro-industriels sont si forts qu'ils justifient des programmes d'armement sans aucun intérêt, si ce n'est de maintenir des équipes d'ingénieurs, techniciens et autres ouvriers en place. Les chars n'ont, par exemple, plus aucune raison

d'exister à notre époque. Pourtant, les militaires soutiennent ces programmes, qui font vivre rien qu'en France des milliers de personnes.

Les militaires invoquent les batailles de chars dans les plaines de l'Europe, susceptibles de redevenir un jour d'actualité. Rien de plus mensonger. Demain comme aujourd'hui, les chars à la pointe de la technologie devront affronter des missiles antichars portés par des fantassins ou largués par des avions. Or ces projectiles coûtent de moins en moins cher (moins de 50 000 francs français) tandis que le coût des chars augmente (plus de 30 000 000 francs français). Dans ce contexte, la durée de vie du char le plus élaboré ne dépasse pas quelques dizaines de minutes.

Pour justifier des dépenses pharaoniques, les lobbies militaro-technologiques se fabriquent également des adversaires fictifs. En 1992 et 1993, les Russes ont vendu aux Iraniens plusieurs sous-marins classiques (à propulsion diesel-électrique) de la classe Kilo. Ces engins (de 3 000 tonnes en plongée) ont été lancés en 1979 par les Soviétiques pour patrouiller aux abords des bases nucléaires américaines. L'amirauté des États-Unis a profité de cet achat iranien pour expliquer que les Kilo étaient extrêmement dangereux.

Pourquoi cette révélation tardive ? La marine américaine ne savait plus quoi faire de sa quarantaine

de sous-marins d'attaque nucléaire de la classe Sturgeon et de ses 64 Los Angeles. Ce nombre extraordinaire ne se justifiait que pour pister en permanence les sous-marins nucléaires soviétiques. Or depuis quelques années, les Soviétiques n'alignent plus qu'une dizaine de sous-marins opérationnels. Pas de chance, car à la même époque, la construction des Sea Wolf, la dernière génération de sous-marins, commençait aux États-Unis.

Pour l'armée américaine, la vente des Kilo aux Iraniens fut donc une bénédiction. La rhétorique de la menace suprême pouvait reprendre du service. Or les Kilo iraniens ne présentent aucun danger en cas de conflit. Les Los Angeles auraient tôt fait de les transformer en lieux de villégiature pour poissons exotiques.

De toute façon, l'utilisation des sous-marins dépend en grande partie de la fourniture de logistique et de pièces de maintenance par les Russes. Sans assistance, ils ne sont pas opérationnels. D'autant que ces engins ont une durée de vie bien plus faible que leurs homologues occidentaux.

Des programmes efficaces, il en existe. Mais dans un concert de désinformation, il est difficile de distinguer les gadgets technologiques des engins indispensables. La mystification du piratage informatique ou des satellites d'observation, entretenue par les médias, en est le brillant exemple.

D'un autre côté, on évoque à peine les petits avions télécommandés, comme les drones, qui rendent des services incommensurables à l'armée israélienne.

"Un coup d'État sera forcément connu des services secrets."

Faux

Les moyens de renseignement des services secrets sont moins efficaces qu'on le croit. La surveillance continue d'une seule personne réclame la mobilisation d'une vingtaine d'agents. L'écoute téléphonique permanente et la pause de micros nécessitent une demi-douzaine de personnes pour analyser les informations. Pour enlever quelqu'un, il faut une douzaine d'intervenants, d'abord pour connaître ses habitudes, puis pour l'opération proprement dite.

Par ailleurs, via le réseau Internet, les ordinateurs les plus simples permettent d'échanger des informations cryptées qu'il est théoriquement impossible de décoder. Dans ce cas, l'écoute devient carrément caduque.

Les actions des services secrets réclament une main-d'œuvre qualifiée et importante ; elles demandent énormément de temps et d'argent.

Agir à grande échelle implique dans les faits l'instauration d'un État policier, comme l'ancienne

Allemagne de l'Est. Rappelons que la police politique de ce pays s'est totalement disloquée dès la chute du mur de Berlin.

"Les satellites permettent de repérer la mise en place d'actions subversives."

Faux

Les satellites d'observation se contentent de photographier le terrain sur différentes fréquences (optiques, infrarouges ou radars). Ils repèrent les installations et les véhicules militaires, mais n'apportent aucune information sur le déplacement des hommes armés. Ce sont des outils qui suivent semaine après semaine l'évolution des infrastructures ou de l'agriculture dans certains pays, comme la Colombie pour les cultures de coca.

Les satellites d'observation, que l'on tente de faire passer pour les outils stratégiques sans lesquels aucune action n'est possible, servent surtout à maintenir en activité des équipes d'ingénieurs.

Les groupes subversifs ont beaucoup plus à craindre des avions de surveillance américains (les AWACs), qui détectent les appareils volants, ainsi que des radars MTI, capables d'indiquer la position instantanée de tous les véhicules terrestres. C'est avec ce type d'engins stratégiques que les États-Unis luttent contre le trafic de drogue ou l'immigration

clandestine.

“Les téléphones portables sont un atout important pour les terroristes.”
Faux

Les terroristes ont intérêt à ne pas utiliser d’appareils sans fil, car les dispositifs d’écoute électronique détectent toutes les sources de rayonnement électro-magnétique, c’est-à-dire les radars, les stations de radio et télédiffusion, les talkies-walkies ainsi que les téléphones portables… C’est d’ailleurs parce qu’il utilisait un téléphone cellulaire que le trafiquant de drogue colombien Pablo Escobar fut localisé.

“Les États ont renoncé aux armes chimiques pour des raisons humanitaires.”
Faux

Les armes chimiques sont en fait très peu efficaces, car les gaz se dispersent au gré du vent et s’éparpillent inutilement. Les pertes de produits sont énormes. Seuls quelques dixièmes de pour cent sont effectivement utiles. Les armées modernes ont donc finalement renoncé à leur emploi.

D’autant que les années 80 ont vu l’arrivée des armes à fragmentation, bien plus efficaces que les

armes chimiques. Ce sont des containers remplis de centaines de grenades et lancés par des avions, des missiles de croisière, des roquettes ou des obus. Avec de telles armes à leur disposition, il est facile pour les militaires de renoncer aux armes chimiques en se montrant sensible aux arguments humanitaires.

"L'efficacité des systèmes de détection de cibles marche tout le temps"

Faux

Par mauvais temps, temps couvert, forte fumée, forte humidité, brouillard, tempête de poussière ou de sable, aucune arme à guidage terminal n'est réellement efficace. Dans de telles conditions météorologiques, les systèmes de désignation et d'acquisition de cible des avions (tels que le F 117 – avion invisible –, F 15E, F 111F, A 6E, F 16, F 18, A 10) s'avèrent inopérants. Durant la guerre du Golfe, par exemple, seules les attaques par temps clair furent précises.

Néanmoins, les systèmes de détection de cible sont des instruments incontournables aujourd'hui, en particulier pour attaquer des camps terroristes dissimulés en montagne (Afghanistan, Bosnie). Comparées aux bombes classiques, les armes à guidage terminal sont plusieurs centaines de fois plus efficaces. Lors de la guerre du Golfe, 43 % des

objectifs furent détruits par des armes à guidage terminal, alors qu'elles ne représentaient que 7 % des munitions utilisées.

Cependant, ces systèmes coûtent cher (plusieurs millions de francs pour le haut de gamme). Il faut donc que les objectifs se justifient économiquement, c'est-à-dire que le rapport entre les dégâts causés et le coût de l'opération doit être le plus élevé possible. (cf. "Les vraies et fausses cibles des terroristes").

"*Les systèmes de missiles antiaériens sont caducs.*"

Vrai

Le concept même de sites mobiles de missiles antiaériens est aujourd'hui caduc. Quand l'adversaire fait preuve de méthode et d'organisation, même les matériels dernier cri français (crotale NG), suisse (ADATS) et russe (SA-11 et SA-15) sont peu efficaces. Les techniques des avions de combat sont en effet parfaitement rodées, réduisant à néant l'efficacité des missiles antiaériens.

Dans une première étape, les avions de reconnaissance électronique observent la zone ennemie à une centaine de kilomètres de distance. Ils localisent les radars, déterminent la "signature" des faisceaux radars, et en déduisent le type de système impliqué. Lorsque les installations sont au cœur d'un

territoire ennemi, ce sont de petits drones (des avions à pilotage automatique, ayant une structure d'ULM) munis de détecteurs de radars qui sont envoyés. Beaucoup sont abattus, mais leur coût de fabrication est cinq à dix fois inférieur à celui d'un missile antiaérien. D'autre part, pour l'interception des drones, les radars doivent être allumés, ce qui donne une information supplémentaire sur l'emplacement et la nature du site.

Dans une deuxième étape, les avions de reconnaissance électronique localisent les sites, avec une précision de quelques centaines de mètres.

Dans une troisième étape, les sites de missiles sont attaqués, soit par des commandos parachutés ou héliportés à moins d'une dizaine de kilomètres des radars, soit par des hélicoptères antichars tirant leurs missiles à 3 ou 4 km de distance, soit par des avions d'attaque larguant leurs missiles à distance de sécurité (12 km), soit enfin par des avions munis de missiles antiradars qui se dirigent vers la source des faisceaux radars.

L'efficacité de cette démarche est redoutable. Pour preuve, l'armée de l'air israélienne perdit 80 avions de combat lors des trois premiers jours du conflit du Yom Kippour à cause des missiles antiaériens. Moins de dix ans plus tard, en 1982, durant la guerre du Liban, 90 % des batteries de missiles antiaériens syriennes furent anéanties pour

une perte totale de… 2 avions. Dans ce dernier conflit, les Israéliens utilisèrent les techniques d'attaque des avions de combat.

Les missiles antiaériens ont pourtant connu leur âge d'or, pendant les années 70, et en particulier après la guerre du Yom Kippour, en 1973. Avant cette date, la maîtrise aérienne était tout simplement synonyme de maîtrise du champ de bataille. Les Israéliens, conscients de cet état de fait, mirent en place une force aérienne qui était et reste la plus efficace au monde.

Après les échecs dus à la prédominance des Israéliens, les Égyptiens investirent massivement dans des sites mobiles de missiles antiaériens (comme les SAM-6 soviétiques) qui accompagnaient les unités terrestres lors de leur progression.

Durant la guerre du Yom Kippour, les Israéliens perdirent plusieurs dizaines d'avions de combat pendant la première journée du conflit. En perdant la maîtrise des airs, les Israéliens se retrouvèrent en mauvaise posture. Il fallut une semaine pour que les pilotes développent de nouvelles manœuvres d'évitement des missiles, et surtout pour que du matériel de brouillage, prêté par les États-Unis, aveugle les radars ennemis. Mais la grande leçon de ce conflit fut l'efficacité des systèmes de missiles antiaériens. Leur commerce devint florissant et tous les pays, sans exception, s'équipèrent de ce type

d'armes.

Les missiles antiaériens s'avèrent aujourd'hui caducs, car les États assurent désormais leur défense à l'aide d'instruments plus performants :

– les missiles air-air à moyenne portée (MICA français ou AMRAAM américain) ;
– les missiles antiaériens portables (Stinger américain, Mistral français ou SA-14 russe), indécelables en raison de leur taille ;
– les missiles sol-air à longue portée (Patriot américain, Aster français ou SA-10 et SA-12 russes), capables d'abattre des cibles (avions ou missiles) situées à plus de 50 km.

Les sites convenant à ce type de missile sont certes vulnérables, mais ils interceptent notamment les missiles balistiques tactiques.

"Le concept de bombardements massifs date de la deuxième guerre mondiale."

Vrai

Le concept de bombardement stratégique date du 21 janvier 1943, par décision commune du Président américain Franklin Roosevelt et du Premier Ministre britannique Winston Churchill.

Cette technique a l'avantage de porter le feu largement au-delà de la ligne de front.

Les objectifs étaient par ordre de priorité :
– les chantiers de construction de sous-marins ;
– les usines de fabrication d'avions et de moteurs ;
– les axes routiers (ponts) et ferroviaires (gares) ;
– les raffineries pétrolières ;
– les industries de base (chimie des explosifs, roulements à bille, etc.).

Une des premières missions réussies fut le bombardement du centre de construction de sous-marins de Vegesack par une centaine de bombardiers (B-17 et B-24), le 18 mars 1943. Ils larguèrent 530 bombes de 450 kg chacune. Pour l'anecdote, la production fut peu affectée par cette action. Néanmoins, ce type d'intervention s'accentua jusqu'à la fin de la guerre. Fin juin 1943, 35 000 tonnes de bombes avaient été larguées sur une quinzaine de sites. Plus de 600 bombardiers furent détruits par la défense antiaérienne ennemie. Durant la grande semaine des bombardements de février 1944, 3 300 sorties permirent le largage de 6 000 tonnes de bombes.

Une des clefs de la victoire alliée résida dans la capacité industrielle de compenser, chaque semaine, la perte d'une centaine de bombardiers. L'Allemagne ne disposant pas de bombardiers lourds, le Royaume-Uni et les États-Unis furent à l'abri des armes

allemandes. À l'exception des V1 et V2, dont la médiocre précision (1 ou 2 km) réduisait l'efficacité militaire à néant.

Dès 1942, la zone d'action de l'Allemagne se limitait à la ligne de front des combats, contrairement à celles des Anglais et des Américains. À partir de ce moment, la défaite des Nazis était inéluctable.

"Pour détruire un AWAC, Tom Clancy préconise de faire suivre à un hélicoptère un train à grande vitesse. Est-ce une bonne idée ?"

Non

L'ouvrage Dette d'honneur de Tom Clancy, retraçant un conflit entre le Japon et les États-Unis, est une mine de détails technologiques réalistes. Dans une des scènes principales, le célèbre écrivain américain décrit la destruction d'un AWAC japonais par un hélicoptère américain Comanche. Pour ce faire, l'hélicoptère s'approche de l'AWAC et largue des missiles antiaériens. Pour ne pas apparaître sur l'écran de surveillance, le pilote du Comanche suit un train à grande vitesse au ras du sol. De cette manière, le radar ne voit pas l'hélicoptère, étant incapable de discerner deux cibles aussi proches.

Il est fortement déconseillé de suivre cette procédure.

Les radars de l'AWAC fonctionnent suivant un mode dénommé "pulse Doppler" qui classe les cibles en fonction de leur vitesse. Ces radars sont munis de filtres qui éliminent les cibles immobiles (c'est-à-dire le sol) ou lentes (voitures). Tom Clancy pense donc qu'un hélicoptère qui suit un train grande vitesse ne peut pas être détecté. Ce qui est vrai, mais à une exception près, et elle est de taille : un hélicoptère ne laisse pas une trace, mais deux sur l'écran radar. La première correspond au corps de l'hélicoptère, l'autre aux pales du rotor. Les pales sont en effet d'immenses hélices qui atteignent en bout d'aile une vitesse de 1 000 km/h. Le décalage Doppler est alors celui d'un objet qui atteint presque la vitesse du son. En survolant le train, si la cellule de l'hélicoptère échappe à l'AWAC, les pales sont à coup sûr détectées par l'ordinateur de bord. L'hélicoptère n'est donc pas un bon instrument pour approcher un AWAC.

A priori, le même problème se pose pour tous les avions à hélices. En fait, la taille réduite des hélices des ULM (diamètre d'un mètre, contre huit pour un hélicoptère) les rend presque indétectables dans le fouillis des échos radars que renvoie le sol.

"La destruction de ses moyens de production est une catastrophe pour un pays."

Faux

Un exemple. Le Nigeria, pays producteur de pétrole, possède quatre raffineries gérées par le secteur public. Ses unités de production ont des coûts de fonctionnement très élevés. Le FMI (Fonds Monétaire International) incite le gouvernement du Nigeria à les fermer. Selon les experts, ces fermetures feraient économiser 100 000 000 dollars au pays, grâce à des importations de produits raffinés bien moins chers. Bref, une attaque dirigée contre les raffineries du pays, loin de lui causer des dommages, renforcerait l'efficacité du pouvoir en place.

"Les marchés financiers sont les meilleures cibles de déstabilisation pour les groupes terroristes."

Faux

Un groupe terroriste qui tente une action de subversion à grande échelle n'a aucun intérêt à déstabiliser le système boursier.

Toute attaque contre les salles de bourse, contre les informateurs des agences de presse qui véhiculent les informations boursières ou contre les analystes financiers serait tout simplement contre-productive. Les marchés boursiers offrent en effet des possibilités de financement inégalées, peut-être plus rentables que l'industrie de la drogue (cf. "Le financement des groupes terroristes"). Il serait donc

dommageable de s'aliéner les gigantesques sommes d'argent que brassent les places boursières.

"De nombreux génies de l'informatique détournentdes sommes d'argent importantes."

Faux

Le piratage informatique est certes un thème en vogue, mais il s'avère très peu efficace comme source de financement.

La France estime que chaque année, environ dix milliards de francs sont perdus à cause de sinistres informatiques. Cette somme est impressionnante, mais elle englobe les effets induits, comme l'immobilisation d'un service à cause d'une panne d'ordinateur.

À l'origine de ces sinistres : la malveillance interne et externe des gens, les virus, le vol de matériel…

La part des détournements de fonds dus au piratage informatique à proprement parler est nulle ! Ou presque…

Si l'on excepte les situations où les pirates ont bénéficié d'une aide interne, il n'existe, à travers le monde, que quelques exemples de détournement informatique d'une grosse somme d'argent. Les piratages informatiques les plus réussis qui défraient la chronique sont des opérations d'atteinte à

l'intégrité des fichiers informatiques. Dans la majorité des cas, cela consiste simplement à recopier un logiciel sur son ordinateur et à l'exploiter sans payer les droits d'utilisation.

Lorsque l'on parle de fraude informatique et de ses conséquences économiques, c'est de piratage de logiciels qu'il s'agit. La facilité de les dupliquer amène à estimer qu'un utilisateur d'ordinateur sur deux possède (parfois malgré lui) des programmes obtenus en dehors du strict cadre légal.

Le seul cas de piratage informatique ayant permis un gain financier important évoqué en France n'est connu que de la communauté des spécialistes de la sécurité bancaire. Vers la fin des années 80, une équipe d'électroniciens, probablement avec l'aide d'un ancien technicien de France Télécom, détourna des fonds de la Banque de France.

Dans un premier temps, ces pirates branchèrent des écoutes sur des lignes de communication de la Banque de France. La mise sur écoute consista simplement à placer un anneau de détection autour des lignes de communication, dans les sous-sols de la banque, afin d'analyser les transmissions. Les lignes où transitaient les communications téléphoniques et les télécopies furent mises de côté. Seules les lignes où passaient des données numériques retinrent l'attention des pirates. Qui plus est, les électroniciens ne s'intéressèrent qu'aux

lignes cryptées et quasiment indéchiffrables.

Il peut sembler étonnant d'écouter uniquement des communications incompréhensibles, mais les pirates avait de bonnes raisons pour cela. En fait, ils remarquèrent que chaque dévaluation du franc était précédée par une intensification des communications cryptées avec la Banque de France. Ils placèrent donc une station d'observation électronique qui détecta les augmentations de volume des données. Ces informations furent utilisées durant des mois pour spéculer contre le franc.

Un responsable bancaire fit remarquer lors d'un entretien privé "qu'il valait mieux que les candidats au piratage n'en sachent pas trop sur ce type d'affaire, et qu'ils continuent à dépenser leur énergie sur les réseaux où il y a peu d'argent à gagner".

En tout cas, cet exemple montre que le pouvoir ne découle pas d'une maîtrise pointue des hautes technologies, mais de leur utilisation adéquate.

"Aujourd'hui, il est extrêmement facile d'intercepter les lignes de communication d'une grande banque."

Faux

De l'extérieur d'une banque, on ne peut se brancher ni sur les lignes de communication numériques, ni sur les fils téléphoniques reliant les

diverses succursales entre elles. Ces lignes transportent en effet des milliards de données provenant de centaines, voire de milliers, d'ordinateurs. Ce sont des lignes multiplexées, à haut débit (2 Mégabits/seconde ou plus), où se mélangent plusieurs lignes à bas débits (64 Kilobits/seconde).

Avant de pirater quoique ce soit, il faut donc démêler cette pelote qu'est la ligne multiplexée. Un démultiplexeur, c'est-à-dire un gros ordinateur muni de programmes de télécommunication spécifiques, est alors nécessaire. Mais une telle machine coûte cher et n'est pas accessible aux particuliers. Autant donc abandonner l'idée d'en faire descendre une dans les égouts d'une grande capitale occidentale.

Si on ajoute à cela la facilité pour les utilisateurs de crypter les informations transitant sur les lignes de communication, et la nature des câbles haut débit (fibres optiques ou coax), il est raisonnable de renoncer à intercepter les lignes de communication d'une grande banque.

La seule solution consiste à se brancher sur la ligne de l'utilisateur final. Il faut pour cela être à l'intérieur de la banque.

"Les moyens de lutte des États contre le blanchiment de l'argent sont inexistants."

Vrai

Il n'existe pas de lutte réelle possible contre le blanchiment d'argent. Dans certains pays, le blanchiment n'est même pas un délit. C'était notamment le cas de l'Allemagne jusqu'en 1992.

D'ailleurs, il n'existe pas d'argent "sale", il y a simplement des opérations contraires aux lois bancaires d'un pays. Or il existe suffisamment de possibilités sur le circuit financier international pour ne pas avoir besoin d'enfreindre les règles. L'argent n'est donc "sale" que par l'incompétence des responsables financiers chargés du blanchiment.

En fait, la majorité des actions de lutte contre le blanchiment porte sur les erreurs commises lors des transferts d'argent. Par exemple, la banque luxembourgeoise BCCI accumula des erreurs grossières de gestion comptable. Elle fit faillite et fut accusée de blanchiment d'argent illicite. En deux phrases, les dirigeants des succursales françaises sont tombés non pas en raison du blanchiment, mais pour le non-respect des règles bancaires imposées par le pays. La banque BCCI avait par exemple fusionné plusieurs comptes-clients en un seul, et contacté directement les trafiquants de drogue colombiens.

Les institutions spécialisées dans la lutte contre le blanchiment éprouvent donc les plus grandes difficultés à débusquer les groupes compétents et organisés.

Au sommet des Sept Pays les plus industrialisés, à

Paris, en 1989, le Groupe d'Actions Financières International (GAFI) fut mis en place. Mais ce groupe de travail ne peut pas proposer de mesures efficaces tant que les paradis fiscaux seront intégrés dans la finance internationale. Les seules mesures à prendre consistent en un contrôle drastique des déplacements d'argent liquide. Cette proposition révèle en soi l'impossibilité effective de lutte contre le blanchiment.

En France, une seule cellule spécialisée, la TRACFIN (Traitement du Renseignement et de l'Action contre les Circuits FINanciers clandestins), possède les effectifs, les moyens et les compétences nécessaires à la lutte contre le blanchiment d'argent.

L'efficacité de ce groupe (de quelques dizaines de membres) résulte en son pouvoir unique de lever les secrets bancaires et d'avoir accès à toutes les informations administratives, bancaires, et commerciales. En revanche, il ne communique ces informations à aucun service, ni de police, ni des impôts.

"Pour transporter du matériel illicite (armes, drogue) par avion, le survol de la mer est plus dangereux que celui de la terre."

Vrai

Le survol de la mer est toujours dangereux, car les

avions de surveillance ont un fonctionnement propre à la surveillance maritime. Sur mer, toutes les réflexions radars sont analysées. Au-dessus de la terre ferme, seuls les objets dont la vitesse est supérieure à 160 km/h sont pris en compte.

La raison est fort simple : les avions de surveillance, tels que l'AWAC américain, possèdent une visibilité du sol importante. Ils détectent donc de nombreux véhicules (voitures, camions, trains…) qui saturent le système. En revanche, au-dessus des flots, tous les objets sont intéressants puisqu'il s'agit de bateaux, quelle que soit leur vitesse.

De même, il faut voler à moins de 30 m au-dessus du sol. Car à cette altitude, les échos de l'avion ou de l'hélicoptère se mélangent à ceux des véhicules terrestres. De plus, les ordinateurs qui analysent les signaux reçus par les radars retiennent tous les appareils, quelle que soit leur vitesse. Pour un radar, être à moins de 30 m d'altitude équivaut à être au sol.

"Les bouteilles que lancent les manifestants sur les forces de police ne sont pas des cocktails Molotov."

Vrai

Contrairement à la croyance populaire, les bouteilles d'essence enflammées que les manifestants lancent sur les forces de l'ordre ne sont

pas des cocktails Molotov.

Les vrais cocktails Molotov furent largement employés pendant la seconde guerre mondiale pour détruire les chars allemands. La technique était simple, efficace et terriblement dangereuse. Des groupes de deux ou trois personnes s'approchaient à quelques mètres des chars et lançaient des bouteilles non enflammées. Le liquide incendiaire s'infiltrait alors à l'intérieur de l'engin. Une dernière bouteille, enflammée, était lancée quelques minutes plus tard, transformant le char en un véritable brasier.

Il existe un grand nombre de recettes pour réussir un cocktail Molotov. Une variante consiste à mélanger deux tiers d'huile de moteur usagée et un tiers d'essence. Il faut ensuite ajouter un peu de glycérine et de copeaux de savon. La bouteille doit être hermétiquement fermée et ne pas contenir d'air. Pour l'enflammer, on colle un bâton de bois à la bouteille à l'aide d'un ruban adhésif. On allumera un bout de chiffon ou de carton enroulé autour du bâton le moment venu.

Une méthode plus subtile consiste à introduire de l'acide sulfurique dans la bouteille, entourée ensuite de chlorate de potassium. Lorsque la bouteille se brise, la réaction entre le chlorate de potassium et l'acide sulfurique entraîne la combustion de l'ensemble. Les esprits vicieux ajoutent des morceaux de pneu finement broyés. La solution

dégage une chaleur intense, difficile à éteindre.

Attention ! Un tel liquide incendiaire est dangereux à manipuler. Il ne faut sous aucun prétexte tenter d'en fabriquer. Les risques d'accident sont élevés. L'acide sulfurique peut réagir avec les impuretés de l'essence ou de l'huile de vidange, et enflammer spontanément l'ensemble.

"Les lance-flammes servent à asphyxier l'ennemi."

Vrai

L'objectif du lance-flammes n'est pas de brûler vivants les combattants, mais de consumer l'oxygène de l'air pour les asphyxier. Durant la guerre du Pacifique, les Marines étaient équipés de lance-flammes (Ronson M1) destinés à l'attaque des bunkers. Le mode d'utilisation consistait à projeter de l'essence non enflammée à travers les ouvertures, puis à y mettre le feu.

"La vente de plutonium par les pays de l'ex-URSS est extrêmement dangereuse pour la sécurité des États occidentaux."

Faux

Si les républiques de l'ex-URSS semblent représenter des fournisseurs compréhensifs pour les

acheteurs disposant de quelques millions de dollars, que peuvent faire des terroristes avec quelques centaines de grammes de plutonium ? À vrai dire, pas grand-chose.

Avec de telles quantités, pas question de réaliser une bombe nucléaire, même miniature : les lois de la physique nucléaire sont là pour contrecarrer ce type de projet. Il faut au moins une dizaine de kilos de matière fissible (uranium fortement enrichi en isotope 235 ou plutonium).

De plus, il faut dépasser la masse critique de matière fissible lors de l'explosion. La masse critique n'étant pas atteinte, la réaction en chaîne n'est pas suffisante pour emballer le plutonium et obtenir une émission explosive d'énergie (c'est-à-dire une explosion nucléaire). D'autre part, le plutonium n'est pas particulièrement radioactif. Les risques d'irradiation sont faibles.

Enfin, fabriquer une bombe nucléaire est un exercice difficile et coûteux. Des livres entiers concernent la fabrication des bombes nucléaires. Ce n'est pas sans raison que seulement une dizaine de pays maîtrisent la conception et la fabrication de telles bombes.

Bien sûr, une action terroriste mettant en jeu du plutonium présente un danger. Notre propos est plutôt de dire que l'effet obtenu sera disproportionné par rapport à l'effort déployé pour fabriquer une bombe nucléaire.

PARTIE 2

LE FINANCEMENT

DES GROUPES TERRORISTES

CHAPITRE 1

MANIPULATIONS BOURSIÈRES

Les marchés financiers correspondent parfaitement aux attentes d'un groupe terroriste en mal de financement et prêt à mener des actions illégales.

Pour gagner à coup sûr, il faut manipuler le marché, c'est-à-dire mener une opération qui fera varier le cours d'une action.

Une opération terroriste (élimination de dirigeants, menace sur un client, destruction d'un centre de production, sabotage des connexions électriques ou téléphoniques…) peut tout à fait faire baisser le cours de l'action d'une entreprise. Il suffit ensuite de jouer à la baisse, de vendre des actions (à 50 F par exemple) avant l'opération puis de les

racheter (40 F). Le bénéfice sera de 10 F par action.

Mais sur quels produits financiers faut-il agir ? Pour cibler les opérations à effectuer, nous expliquons quels sont les véritables acteurs des marchés financiers et passons en revue les avantages et inconvénients des principaux produits existants.

Les acteurs des marchés financiers

La bourse mondiale est constituée de quelques dizaines de places boursières. Dans chacune, acheteurs et vendeurs échangent des produits (actions, obligations, options…) sous la surveillance d'une police des Bourses qui veille au respect des règles en vigueur.

Ces intervenants sont tous ceux qui gèrent de grosses sommes d'argent : les banques ; les caisses de retraites ; les assureurs et les mutuelles qui s'occupent des contrats d'assurance ; et enfin, les institutions financières qui placent les portefeuilles des épargnants… C'est-à-dire les Mutuals Funds aux USA, United Trusts aux Royaume-Uni, SICAV (Société d'Investissements à Capital Variable) et FCP (Fonds Commun de Placement) en France.

Les principaux mouvements de capitaux mondiaux sont dus essentiellement à quelque 200 gros intervenants, essentiellement anglo-saxons ou japonais. Ce sont eux qui prêtent de l'argent aux

États pour combler leur déficit public. Leur pouvoir financier dépasse largement celui des États, gouvernement américain inclus. Un grand nombre disposent pour investir de plus de cent milliards de dollars.

Cette puissance financière s'est vue récemment accrue par la quasi-faillite des grands États. Les États vivent en effet depuis des années au-dessus de leurs moyens, creusant des dettes de plus en plus importantes. Plus un seul État ne dispose aujourd'hui d'une puissance financière comparable à celle de ces 200 institutions.

L'Arabie Saoudite, par exemple, vit ses revenus plonger à cause de la politique des quotas de production de l'OPEP et de la chute du prix du baril de pétrole. En même temps, le contexte géopolitique de l'après-guerre du Golfe l'obligea à acheter massivement du matériel militaire américain et anglais, pour "remercier" les forces alliées et renforcer sa défense.

Même phénomène au Japon. Le tremblement de terre de Kobe causa des dégâts évalués à près de cent milliards de dollars. Le gouvernement japonais a besoin de toutes ses ressources pour reconstruire la ville.

Quant à l'Allemagne, la réunification absorbe toutes ses liquidités. Début 95, sa dette publique atteignit le niveau de celles de la France et du

Royaume-Uni, soit près de 55 % de son PIB.

Les grands investisseurs suivent de près les analyses des six grandes institutions financières. Ces six banques d'affaires sont Merill Lynche, le Crédit Suisse–First Boston, Morgan Stanley, Lehman Brothers, Salomon Brothers et Goldman Sachs.

Dans les faits, les ordres boursiers ne concernent que quelques dizaines de milliers de personnes de par le monde. Ces acteurs sont les "traders" chargés d'acheter et de vendre les produits, en suivant les recommandations des analystes et de leurs clients.

Ils travaillent dans les salles de marché, c'est-à-dire dans des bureaux où, par téléphone ou liaison informatique, des dizaines de traders passent les ordres d'achat ou de vente, en suivant l'évolution des cours sur les écrans de leurs ordinateurs.

Étant donné les sommes en jeu et la rapidité avec laquelle elles sont engagées, il faut surveiller le travail des traders et avaliser leurs ordres. Cette tâche revient aux "back offices" qui enregistrent les transactions. Ils n'ont aucune capacité de décision, sauf celle de bloquer une transaction si une irrégularité apparaît.

Les produits de base des marchés financiers

Il existe deux types de produits que s'échangent les boursiers sur les marchés financiers :

– les produits dits “de base”. Ce sont les actions, les obligations, les obligations à haut risque (ou “junks bonds”) et les monnaies ;
– les produits dérivés. Ce sont les marchés à terme et le marché des options.

Les produits de base

Les actions

Les actions sont les parts d’une société. Si la valeur d’une société monte, ses actions montent. Les actions redeviennent depuis peu des produits intéressants pour spéculer.

Les obligations

Les obligations sont les parts d’un emprunt émis par une société ou un organisme. Contrairement aux actions, leur valeur est indépendante de la santé de l’emprunteur. Tels les prêts, leurs conditions sont fixées à l’avance et les risques sont faibles.

La valeur des obligations ne dépend que des taux d’intérêt. Si les taux d’intérêt montent, le client est tenté de vendre pour placer son argent dans de nouvelles obligations dont les taux d’intérêt sont plus bas.

Les obligations se prêtent donc peu à la

spéculation, car leur valeur est stable et ne fluctue pas en temps réel.

Les “junks bonds”

Les junks bonds (traduction : obligations “pourries”) sont des obligations à haut risque. Ils furent l’instrument privilégié des “golden boys” aux États-Unis dans les années 80. Ce sont des obligations avec un taux d’intérêt très élevé, mais présentant un risque important puisque l’emprunteur n’est pas toujours certain de pouvoir les rembourser.

L’avantage de ce produit est que le spéculateur, en émettant ces junks bonds, peut rassembler plusieurs milliards de dollars. Cet argent sert le plus souvent à effectuer un raid ou une OPA (Offre Public d’Achat), pour prendre le contrôle d’une entreprise en achetant une quantité suffisante de ses actions. Puis le spéculateur, devenu raider, dépèce la société en la revendant par morceaux.

Ce type de vente, appelé vente par appartements, permet de dégager d’importants profits, tout en remboursant, si tout se passe bien, les détenteurs d’obligations. Mais ces opérations sont dangereuses et doivent être effectuées rapidement. Car plus le temps passe, plus l’OPA est difficile à réaliser. Le cours de l’action augmente à cause de l’offre d’achat. Et en même temps, il faut verser des intérêts

importants aux détenteurs d'obligations.

Ainsi, dans le passé, plusieurs protagonistes ont fini en prison. Le fameux raid des années 80, qui porta sur la prise de contrôle du géant du tabac et de l'agroalimentaire Nabisco, se termina en eau de boudin, laissant un manque à gagner de quelques centaines de millions de dollars à ses spéculateurs.

Les OPA montées à l'aide de junks bonds sont aujourd'hui passées de mode. Elles ne sont plus aussi rentables que dans les années 80. Les junks bonds, comme les obligations, ne sont donc plus de bons produits de spéculation.

Les produits dérivés

Le marché à terme

Le marché à terme (future, en anglais) consiste à acheter un des quatre produits de base à l'avance, c'est-à-dire pour un prix et une date fixés à l'avance. Le jour venu, l'acheteur régularise sa situation. Si l'action vaut plus que le prix payé, il est gagnant. Dans le cas contraire, il est perdant.

Pourquoi les autorités boursières ont-elles permis le développement de ce marché spéculatif ? Comme toujours en économie, le marché à terme répond à une demande légitime de la part des investisseurs. Au début des années 70, les parités de change entre les

monnaies qui étaient fixes ont disparu. Les monnaies ont donc commencé à fluctuer. En offrant aux vendeurs la possibilité de vendre à l'avance leurs actions, le marché à terme offrait l'avantage d'être moins dépendant des fluctuations au jour le jour des monnaies. Il permet donc aux entreprises multinationales et surtout aux émetteurs d'emprunts obligataires de se dégager des incessantes variations des taux de change.

Le marché à terme ressemble fort à un jeu de hasard, et attire en nombre les spéculateurs. Pour "aider" le hasard, ceux-ci pipent parfois les dés en influant sur la vie d'une entreprise ou d'un État pour faire varier le cours d'une action.

À Paris, le marché à terme est le MATIF et à Londres, le Liffe.

Le marché à options

Les produits qui remportent tous les suffrages des spéculateurs sont les options. Sur ce marché, il n'est plus nécessaire d'acheter puis de vendre à terme. On verse une somme qui donne droit d'acheter ou de vendre une action à un prix et une date donnés. Les options peuvent être des options d'achat ou des options de vente.

Quelle différence avec le marché à terme ?

Avec un contrat d'achat à terme, l'acheteur est obligé de régler son vendeur le jour venu, et cela quel que soit le prix de l'action. Les pertes peuvent donc être importantes. En revanche, avec une option d'achat, le jour venu, l'acheteur peut soit renoncer à l'action, auquel cas il perd la somme que lui a coûtée l'option, soit il acquiert l'action et dans ce cas il ne verse que le complément.

Dans la catégorie des options, les "warrants" ou bons de souscription donnent le droit d'acquérir une action à long terme et à un certain prix. Les warrants sont utilisés pour deux usages : spéculer et couvrir ses risques.

La plus grande place mondiale des options se trouve à Chicago, au "Chicago board options exchange". À Paris, le marché des options est le Monep, et à Londres le Liffe.

Comment se financer à l'aide de la manipulation boursière ?

Les produits conseillés pour spéculer et donc pour financer une organisation subversive sont les produits dérivés.

Attention, avec ce type de produit, les gains peuvent être importants, mais les pertes aussi. Il est assez courant de perdre l'intégralité de sa mise, et même plus…

En décembre 1994, le Comté d'Orange en Californie perdit plus de deux milliards de dollars avec des produits dérivés et fit faillite. Des écoles, hôpitaux et services municipaux avaient placé leurs fonds dans ce Comté.

De la même façon, la banque Baring Brothers fit faillite à la suite de ses prises de position sur le marché des dérivés de Tokyo.

Néanmoins, le marché à terme et les options sont des jeux à somme nulle. Ce que l'un perd, l'autre le gagne. Sur le marché des actions, tous les intervenants peuvent perdre en même temps, car toutes les actions peuvent baisser simultanément.

Exemples de spéculations que pourrait mener un groupe terroriste.

Ces produits dérivés sont donc parfaits pour manipuler les marchés. Si l'on sait "canaliser le hasard" et initier des baisses des produits, il y a énormément d'argent à gagner. Ces marchés correspondent parfaitement aux attentes d'un groupe en mal de financement et prêt à mener des actions illégales.

Voici deux exemples de spéculation que pourrait mener un groupe terroriste : le premier concernant le marché à terme, l'autre le marché à options.

Sur le marché à terme, un groupe terroriste vend à

terme les actions d'une entreprise (prix : 50 F par action), à travers une société écran située dans un paradis fiscal. Des opérations de subversion sont ensuite menées pour faire baisser le cours de l'action. On pense à l'exécution du directeur général de l'industrie, l'explosion d'un site de production, ou des bruits qui courent sur la baisse du chiffre d'affaires de l'entreprise…

Le jour du règlement, le groupe terroriste achète les actions 40 F pour les revendre 50 F comme prévu par le contrat à terme. Le bénéfice est donc de 10 F par action.

Ce type de spéculation est courant dans le monde boursier. Les manipulations sont généralement non violentes. On fait courir des bruits alarmistes sur une société pour faire baisse son action.

Fin 96, une personne fit ainsi courir des bruits alarmistes sur Eurotunnel. L'agence France Presse reprit la rumeur comme une information. L'agence Reuters exploita à son tour l'information à partir des sources AFP. Les traders, les yeux rivés sur les écrans Reuters, amorcèrent la baisse du titre.

Il fallut plusieurs heures pour que les cours s'inversent et que les informations alarmistes soient démenties par Reuters. Mais, entre-temps, l'initiateur de la manipulation avait largement eu le temps de se dégager et d'empocher une importante plus-value.

L'inconvénient de cette spéculation est que les

gains sont limités à 50 %. Le profit est également limité par la capacité à obtenir des crédits. Comme notre groupe terroriste est certainement un nouveau venu dans le monde boursier, qui se cache derrière une société immatriculée dans un paradis fiscal, le marché à terme lui consentira peu de crédit, limitant d'autant son gain potentiel.

Néanmoins, les marchés à terme sont plutôt des marchés internationaux. La société écran peut passer incognito dans le monde boursier. Le groupe terroriste peut également acheter une société en faillite qui a pignon sur rue dans le monde boursier.

Concernant le marché à options, pour la même industrie, le groupe terroriste achète une option de vente de l'action à 49 F. Le coût de cette option est proportionnel aux variations attendues (par exemple, 20 centimes). Puis, les terroristes organisent des opérations de manipulation qui font baisser le cours à 48 F. Le groupe terroriste vend donc l'option à 1,20 F. L'avantage de ce marché est qu'il n'y pas besoin d'emprunter de l'argent pour spéculer. Le gain peut être de 500 %, alléchant comparé aux gains maximum de 50 % du marché à terme.

Néanmoins, les options sont dans un marché plutôt national, donc plus surveillé. Le groupe terroriste devra faire plus attention pour ne pas être découvert.

CHAPITRE 2

L'INDUSTRIE DE LA DROGUE

L'industrie de la drogue est une activité économique comme une autre, elle répond aux lois de l'offre et de la demande. L'échec des politiques répressives envers le trafic de drogue résulte en grande partie de l'idée que la demande n'existe que parce que l'offre existe. En fait, l'offre n'existe que parce qu'il y a demande. Si l'offre croît, c'est que la demande croît.

Ce type d'industrie est l'activité par excellence des groupes subversifs, et le restera encore longtemps pour des raisons économiques évidentes. La production et l'industrie de la drogue sont des activités extrêmement rentables et offrent un moyen simple de financement inégalé. Rien que pour la

filière colombienne de la cocaïne aux États-Unis, la capitalisation boursière serait de l'ordre de trente à quarante milliards de dollars, le profit annuel de trois milliards de dollars, et les marges de 80 à 95 %.

Si cette entreprise était cotée en bourse, elle se placerait au trentième rang des plus grosses capitalisations américaines, et parmi les dix premières pour les profits.

Le marché n'est pas près de disparaître, car la légalisation complète des drogues n'est pas envisageable. À part le cannabis et ses dérivés (comme le haschisch), une société ouverte et démocratique ne peut envisager de légaliser la diffusion de produits qui induiraient des coûts importants en terme de santé publique et de sécurité (comme l'héroïne, le crack ou les amphétamines). Les États se dirigent plutôt vers une tentative pour restreindre l'usage des drogues légales par des taxes importantes et une interdiction de la publicité.

Les groupes subversifs ont donc là un marché idéal pour financer leurs opérations. D'ailleurs, production de drogue, trafic d'armes et actions terroristes sont intimement liés.

Alors, quelles sont les drogues les plus rentables ? Quelle est la structure de la filière de la drogue ? Quels sont les moyens nécessaires pour réussir dans l'industrie de la drogue ? Comment blanchir l'argent de la drogue ? Quels sont les moyens de transport

pour l'approvisionnement du produit chez les grossistes ? Comment transférer les fonds blanchis en Occident sans éveiller de soupçons ? Voilà les questions auxquelles nous répondons dans ces pages.

Les différents types de drogue

L'opium et l'héroïne

Il existe deux types de drogue :

– les drogues d'origine naturelle. Ce sont les dérivés du pavot (opium, héroïne, morphine), du coca (cocaïne) et du cannabis (haschich) ;
– les drogues de synthèse. Ce sont les amphétamines et leurs dérivés (ecstasy, LSD).

Les dérivés du pavot

Dans la fleur de pavot, l'opium naturel est enfermé sous forme de gouttes végétales. On cueille une centaine de fleurs pour extraire un gramme d'opium. Selon l'ONU, la production mondiale serait de quelques milliers de tonnes par an. De l'opium, drogue traditionnelle de nombreux pays, on extrait trois substances : la morphine, la codéine et l'héroïne. La morphine et la codéine sont les principes actifs de nombreux médicaments pour

lutter contre la douleur. La morphine n'est apparue qu'au début du XIXe siècle.

L'héroïne est extraite de la morphine par mélange avec de l'anhydride acétique. D'un kilo d'opium, on obtient après transformation cent grammes d'héroïne. L'héroïne est la plus rentable des drogues naturelles. Son prix au kilogramme est dix fois plus important que celui de la cocaïne. En revanche, la demande du marché est beaucoup plus forte pour la cocaïne.

Les dérivés de la coca : cocaïne et crack

L'aventure de la cocaïne commença avec un chimiste allemand qui, en 1857, isola la substance active de la feuille de coca. La notoriété de la cocaïne fut établie par la fantastique réussite de deux boissons fortifiantes, le vin Mariani et le Coca-Cola. La fameuse boisson gazeuse était en effet à base de cocaïne et de caféine. Depuis, elle fut décocaïnisée.

La cocaïne est un neurostimulant au même titre que les amphétamines. Le crack est aussi de la cocaïne, mais non raffinée, qui se fume. Ses effets sont dévastateurs sur le système nerveux.

Pour raffiner la cocaïne, il faut utiliser des produits chimiques de raffinage comme le kérosène, l'acétone, l'éther et le permanganate de potassium.

Traditionnellement, la cocaïne provient

d'Amérique centrale. La Colombie et la Bolivie en sont les principaux pourvoyeurs. La demande ne cesse d'augmenter. Selon l'ONU, la production serait actuellement de quelques centaines de tonnes par an.

Le cannabis et ses dérivés

Pour financer un groupe subversif, le cannabis offre beaucoup moins d'avantages que l'héroïne et la cocaïne. Le prix de gros est en effet cent fois moins important que pour les autres drogues. D'autre part, un grand nombre de consommateurs cultivent la plante pour leur propre consommation. Néanmoins, selon l'ONU, la production mondiale de cannabis est la plus élevée, avec quelques dizaines de milliers de tonnes par an.

Le cannabis est une plante connue sous de nombreux noms : marijuana, chanvre indien, kif… Ses feuilles sont séchées puis fumées, mélangées à du tabac. Sous cette forme, cette drogue, illégale dans de nombreux pays, s'apparente au tabac. La dépendance est d'ailleurs moindre que celle induite par l'alcool. Le risque d'overdose n'existe pas et les accidents médicaux sont rares, car les feuilles ne sont pas coupées avec des produits chimiques.

Lorsque les gouvernements parlent de légalisation de la drogue, leur discours ne concerne que le cannabis.

Cependant, les dérivés de la plante sont plus dangereux. La résine (également appelée haschich) ou l'huile de cannabis présentent de réels dangers pour la santé dans la mesure où le principe actif du cannabis, le THC (ou tétrahydrocannabinol), y est présent sous forme concentrée.

Les drogues de synthèse : ecstasy, LSD

Pour financer une opération subversive, les drogues de synthèse offrent l'avantage de se passer d'agriculteurs et de terres cultivables, au profit d'industriels de la chimie. Néanmoins, la technicité requise est plus élevée et nécessite la mise en place d'unités de production de chimie fine. Les techniques sont strictement celles de l'industrie pharmaceutique.

Certains pays élaborent de nouvelles drogues de synthèse, à l'intention d'organisations illégales. Un grand nombre d'experts provenant d'États qui ne peuvent leur offrir de débouchés professionnels et dont la culture ambiante accepte la violence sociale généralisée sont des candidats idéaux à ce genre de trafic. Le Pakistan, la Russie ou le Nigeria représentent quelques exemples de ces "zones grises" favorables au développement des nouvelles drogues de synthèse.

De plus, l'industrie pharmaceutique est

caractérisée par un faible rendement des découvertes : en moyenne, une seule molécule sur 10 000 est médicalement intéressante.

En revanche, pour l'obtention de nouvelles drogues illégales, les contraintes techniques sont moindres, d'où un rendement cent fois plus élevé que dans la recherche pharmaceutique classique. Les amphétamines et leurs dérivés (comme l'ecstasy) sont les principaux membres de la famille des drogues de synthèse.

Le LSD et la phencyclidine ("poudre d'ange") entrent également dans cette catégorie. Mais leurs effets les distinguent des autres drogues. Les hallucinogènes de synthèse ont, sous certaines conditions de production, des effets de "déstructuration sociale". À ce titre, les hallucinogènes de synthèse peuvent être considérés comme des armes de combat plutôt que comme une source de financement.

Le LSD fut synthétisé en 1938 par Albert Hofman, dans les laboratoires Sandoz à Bâle. C'est une substance hallucinogène sans couleur, sans odeur ni goût particulier, donc facile à dissimuler dans les aliments. Elle a été extraite d'un champignon, l'ergot de seigle, connu pour ses effets hallucinogènes.

Les effets du LSD n'ont été découverts qu'en 1943 par Hofman lui-même, à la suite d'une absorption accidentelle par la peau des doigts, puis

par ingestion. En 1977, un chimiste anglais, Richard Kemp, fut arrêté en Angleterre pour avoir produit et vendu de grandes quantités de LSD. Le procès révéla qu'il avait mis au point vers 1970 une nouvelle méthode plus simple et économique de synthèse du LSD. Par un jeu de procédures administratives, la méthode fut rendue publique lors du procès.

L'armée américaine tenta alors d'utiliser le LSD comme arme chimique non mortelle. Une arme idéale, car l'effet hallucinogène est incapacitant et réversible, la durée du phénomène étant de six à huit heures. Mais ce projet ne fut pas concrétisé, les effets par inhalation sous forme de gaz ou de gouttelettes s'avérant infiniment moindres que par ingestion. Le LSD est peu efficace lorsqu'il est répandu dans l'atmosphère.

En revanche, une autre substance psychoactive, la BZ (la quinuclidinyle benzilate), donna de meilleurs résultats pour un usage militaire, car elle peut être répandue à l'aide de bombes aérosols. La BZ est un hallucinogène puissant dont l'effet dure plusieurs jours et entraîne une amnésie, contrairement au LSD.

Une autre substance, la STP, dont les effets sont proches du LSD mais avec une période hallucinatoire s'étendant sur 3 jours, fut synthétisée en 1964 par un chercheur de la société Dow Chemical.

Le problème de la dispersion aérienne d'un agent

chimique incapacitant est celui du dosage : soit la concentration ne suffit pas pour obtenir l'effet désiré, soit elle est si importante que le produit devient mortel. La répartition uniforme de l'agent chimique est également problématique. Les pertes sont donc toujours importantes. Cela explique que les armes chimiques sont difficiles d'emploi et peu efficaces.

Pour une administration par voie orale, le dosage du LSD est de 100 à 300 microgrammes. Cela signifie que 300 g de LSD pur correspondent à plus de deux millions de doses. Mais seulement 0,1 % du LSD ingurgité atteint réellement le cerveau. Le reste est bloqué dans le foie, la rate et les reins.

Un seul médicament peut contrer les effets du LSD : la thorazine, que l'on injecte en cas de surdose de LSD.

La structure économique de la filière de la drogue

La filière de la drogue est divisée en cinq maillons :

– les producteurs de matières premières. Ce sont les agriculteurs pour les drogues naturelles, les chimistes pour les drogues de synthèse. En terme de production agricole, un hectare de pavot donne quelques kilogrammes d'opium. Le prix d'un kilo est de quelques centaines de francs ;

– les producteurs de drogue. Avec un kilo d'opium, on obtient après transformation 100 g d'héroïne. Le coût de production est donc de l'ordre de quelques milliers de francs le kilo ;
– les transporteurs sont en fait les responsables de la logistique. En général, ils sont aussi producteurs ;
– les grossistes maîtrisent à une échelle régionale ou nationale le circuit de distribution. Le kilo d'héroïne se négocie autour d'un million de francs ;
– les revendeurs (ou dealers) sont en prise directe avec les clients. Le kilo d'héroïne se vend autour de dix millions de francs.

Entre le coût de revient pour le producteur et le prix d'achat par le consommateur, il y a un facteur mille. Les profits se concentrent en général sur les producteurs-transporteurs et sur les grossistes. Chacun multiplie le prix par cinq ou dix. Le point fort de cette filière est que la drogue, l'héroïne en particulier, ne vaut rien tant qu'elle n'est pas entre les mains des grossistes. Une saisie d'un kilo d'héroïne dans un aéroport ou un port ne représente qu'un préjudice de quelques milliers de francs, dus au prix de production de la drogue. C'est le prix d'un billet d'avion !

Dans ces conditions, il est logique que les

producteurs-transporteurs ne craignent pas les contrôles douaniers, tant qu'un paquet sur quatre passe à travers les mailles des filets.

Les producteurs-transporteurs sont donc virtuellement intouchables, pour peu qu'ils ne commettent pas d'erreur grave de stratégie économique.

Toutefois, il en va autrement pour les saisies auprès des grossistes qui ont payé la marchandise près d'un million de francs ! Ces derniers constituent le point faible de la filière de la drogue.

Le blanchiment de l'argent de la drogue

La drogue est vendue de la main à la main en liquide, pour ne pas laisser de trace de transaction. Des petits dealers aux producteurs en passant par les grossistes, tout le monde est payé en liquide. Et plus on monte dans le circuit de distribution, plus l'argent liquide se concentre. Les grossistes finissent par disposer de plusieurs millions de francs à la fois. Or il est impossible, dans les démocraties occidentales, d'effectuer des transactions sur de grosses sommes en liquide. Même les succursales des banques européennes situées dans les pays non démocratiques n'acceptent pas de dépôts en argent liquide supérieurs à cent mille dollars. Le fruit d'une vente de quelques kilos de cocaïne pure nécessiterait donc

plus d'une centaine de dépôts successifs ! C'est encore le meilleur moyen de se faire repérer par les services de lutte antidrogue.

Le blanchiment de l'argent consiste à réintroduire cet argent liquide dans le système économique classique. Mais comment ?

La première méthode consiste à prendre le contrôle d'une chaîne de magasins réalisant principalement son chiffre d'affaires en argent liquide : chaînes de restauration rapide, pizzerias, discothèques, casinos, cinémas, salles de spectacle, laveries automatiques…

Il suffit ensuite de déclarer l'argent issu de la vente de la drogue comme un revenu commercial. Il faut cependant veiller à ce que la consommation de matières premières soit compatible avec les déclarations de revenus. Par exemple, une pizzeria qui déclare vendre des centaines de milliers de pizzas mais n'achetant que quelques kilos de farine est rapidement suspectée de trafic.

Ce circuit de blanchiment nécessite donc de posséder un grand nombre de commerces pour traiter des sommes importantes. Les problèmes logistiques sont difficiles à gérer, car il faut toujours veiller à la cohérence des rentrées et des sorties d'argent.

En bonne logique du marché, ce type de blanchiment est devenu une activité indépendante. Les grossistes et les producteurs confient l'argent

liquide aux spécialistes du blanchiment, qui leur retournent une somme d'argent légalisée sur laquelle impôts et commissions ont été prélevés.

La deuxième méthode, certainement la plus efficace, consiste à trouver des banques dans des paradis fiscaux, et à ouvrir des comptes au nom d'une société fictive. Des banques complaisantes, il en existe partout dans le monde, même en Europe.

Quelques règles pour choisir une banque :

- vérifier que le secret bancaire est absolu. C'est le principe des comptes à numéro où le propriétaire est inconnu ;
- la circulation des devises doit y être libre ;
- les liens avec la banque et les financiers occidentaux doivent être importants ; concrètement, le flux d'argent entre le paradis fiscal et les institutions des grandes démocraties doit représenter un pourcentage important des fonds déposés et gérés par la banque ;
- enfin, il faut que les infrastructures de télécommunication et de transport soient suffisantes.

Le transfert des fonds en Occident

Une fois ouverts un certain nombre de comptes dans des paradis fiscaux, il est souvent nécessaire de

transférer les fonds blanchis en Occident sans éveiller de soupçons.

Le trafiquant doit pour cela investir une partie de ses avoirs en placements traditionnels (immobilier, bons du Trésor, bourse…), et une autre partie en se portant garant pour un prêt contracté auprès d'une banque classique, dans le cadre d'un projet commercial ou industriel.

Prenons le cas de l'achat d'un centre commercial. Le trafiquant se présente comme l'instigateur d'une société qui achète un centre commercial. Cependant, comme il ne dispose pas (officiellement) d'argent, il s'associe à des investisseurs, qui sont ses propres sociétés fictives. Dans ce cadre, les investissements en bons du Trésor ou en titres de bourse servent de garantie pour emprunter les sommes nécessaires à l'achat d'un centre commercial.

Les avoirs financiers découlant du centre commercial sont petit à petit reversés à la banque pour couvrir l'emprunt. Au bout de quelques années, le trafiquant de drogue se trouve légalement à la tête d'un centre commercial qu'il lui suffira de vendre. Une partie de l'argent lui reviendra directement et le reste indirectement, à travers ses sociétés fictives.

L'industrie de la drogue, de la production jusqu'au blanchiment de l'argent, nécessite donc la mise en place d'une structure spécialisée importante. Le recours à des spécialistes de divers domaines et

pas seulement chimistes s'impose. Il faut des avocats et des experts connaissant parfaitement les lois en vigueur dans les paradis fiscaux et les pays où se trouvent les grossistes. Il faut fonder une entreprise d'import-export et de location de containers, comme toutes les activités de commerce international. Pour ne pas être repérée, l'entreprise aura une activité licite, qui évite les erreurs importantes.

L'expédition, depuis la Colombie vers Paris, d'un container qui transportait des coffres-forts et des dizaines de kilos de cocaïne en fut une. En effet, la France n'importe pas de coffres-forts de Colombie. Le container fut considéré comme suspect dès son arrivée, et la drogue saisie.

Les moyens de transport de la drogue

Le transport par container, par voie maritime, est le meilleur moyen de faire transiter du matériel illicite entre deux points de la planète. Chaque grand port occidental réceptionne tous les jours plusieurs containers de près de vingt tonnes. Il est matériellement impossible de tous les vérifier.

La principale règle à respecter pour cacher un produit dans un container consiste à entourer l'objet illicite de matériaux de même densité. Par exemple pour des résines de cannabis de densité égale à un, les plastiques ou les liquides usuels conviennent. Pour

les armes, il faut de la fonte ou de l'acier, c'est-à-dire des matériaux de densité sept. L'aluminium est donc à proscrire. C'est le moyen le plus efficace de contrer le seul appareil de vérification existant : le Sycoscan (système de contrôle de containers par rayon X) mis au point par la société Schlumberger.

Si les chiens et leur flair extraordinaire restent un moyen de détection efficace, c'est à mettre au compte de la médiocrité des trafiquants. Pour tromper les limiers, il suffit en effet, sur le lieu de production, de placer les substances illicites dans des sacs en plastique dans lesquels on aura fait le vide, puis de les souder, de recommencer l'opération et de laver soigneusement l'emballage final.

Il existe d'autres moyens de transport : les vedettes hors-bord, les hélicoptères et les avions, qui permettent de passer à travers les mailles des systèmes de surveillance. En vogue un certain temps, les hors-bord sont aujourd'hui technologiquement dépassés. Pour bénéficier de leur principal avantage, la vitesse, les moteurs de hors-bord (de plusieurs centaines de chevaux) doivent tourner à plein régime. Cela se traduit par un rayonnement thermique d'autant plus important que la mer constitue un fond d'images froid, accentuant le contraste.

Les hors-bord ont été supplantés dans cette fonction par les hélicoptères. Ces derniers sont bon

marché. Ils vont plus vite. Et leurs signatures thermique et radar ne sont pas plus importantes, à condition de voler au niveau du sol. Concrètement, cela limite l'altitude de croisière à moins de 30 m, valeur correspondant à la résolution minimale des meilleurs radars de surveillance. Le vol devant s'effectuer de nuit, il faut néanmoins des pilotes bien entraînés et un équipement de vision nocturne (caméra thermique, intensificateur de luminosité, altimètres précis et système de positionnement GPS).

Les avions légers (ULM…) constituent également un bon moyen de transport. Voire le meilleur, car les hélicoptères sont beaucoup plus onéreux et plus visibles que les avions légers. À charge et vitesse égales, les hélicoptères sont plus bruyants. Leurs longues pales forment des surfaces réfléchissantes très visibles pour les avions de surveillance. Le vol de nuit à basse altitude permet aux petits avions d'accomplir la mission de transport à moindre frais.

Finalement, pour transporter des produits illicites autrement que par containers, il faut choisir un avion léger, voler à moins de 30 m au-dessus du sol, avoir une vitesse comprise entre 120 et 160 km/h, survoler de préférence des infrastructures de transport terrestre (autoroutes, rails…), et être équipé d'un système complet de navigation de nuit.

PARTIE 3

LES ARMES DES TERRORISTES

CHAPITRE 1

QUELLES ARMES UTILISÉES?

La plupart des opérations sont à mener sur une cible fixe, occupant une petite surface (moins d'un hectare). C'est le cas d'un bâtiment, une industrie, un navire, une station radar, un site de lancement de missiles…

Pour détruire ces cibles, on dispose d'un panel d'armes concurrentes mais souvent complémentaires. Mis à part les armes légères (pistolets, mitraillettes, fusils…), sept armes s'avèrent particulièrement utiles.

Le canon lourd (155 mm)

Poids d'un obus : 43 kg. Charge militaire : 12 kg. Cadence de tir : 6 coups par minute. Nombre d'obus correspondant à une charge militaire de 600 kg : 50. Portée des tirs : 24 km. Portée d'intervention : quelques dizaines de kilomètres.

Avantages : faible coût.

Inconvénients : le canon est vulnérable ; il est difficile d'envisager de tirer plus de 10 minutes, soit 50 obus sans devoir se déplacer rapidement sur plusieurs kilomètres. La portée d'intervention est également limitée à cause du poids du canon (9 tonnes) et des obus.

Le mortier de 81 mm ou 60 mm, avec lance-grenades automatiques de 40 mm

Quantité maximale d'obus transportable par un groupe de commandos : 600 à 800 kg. Portée de tir : 1,5 à 6 km. Portée d'intervention : 200 km pour le transport par hélicoptère, puis 10 à 30 km à l'aide d'un véhicule léger, et enfin 6 km de portée de tir, soit au total 200 à 250 km.

Avantages : faible coût (quelques centaines d'obus de mortier); portée d'intervention de plus de 100 km.

Inconvénients : rupture de charge à quelques

dizaines de kilomètres de l'objectif ; charge militaire limitée; visibilité du véhicule de transport (hélicoptère).

Le lance roquettes sol-sol

Poids d'une roquette : 112 kg (BM-24 russe)/308 kg (MLRS américain). Charge militaire d'un obus : 46 kg (BM-24)/148 kg (MLRS). Nombre de roquettes par lanceur : 12 (BM-24)/12 (MLRS). Cadence de tir : 12 coups en moins d'une minute. Poids total de la charge utile par lanceur : 552 kg (BM-24)/1 776 kg (MLRS). Portée de tir :11 km (BM-24)/35 km (MLRS). Portée d'intervention : quelques dizaines de kilomètres.

Le lance roquettes air-sol tiré d'hélicoptère ou d'avion

Poids de la charge militaire : 7,25 kg (CRV-7 canadien). Nombre de roquettes par porteur : 76 (4 paniers de 19 roquettes). Poids total de la charge utile par porteur : 551 kg. Portée de tir : 4 km. Portée d'intervention : environ 200 km (hélicoptère) ou 800/1 000 km (avion).

La bombe larguée par avion ou autre

Poids de la charge militaire : 450 kg. Nombre de bombes guidées par avion porteur : 2. Poids total de la charge utile par porteur : 900 kg. Portée de tir maximum : 8 km. Portée d'intervention : 800/1 000 km (avion).

Le missile de croisière à turboréacteur (avec système de navigation mais sans système de guidage terminal)

Structure furtive. Poids total de 1/1,5 tonnes. Vitesse de croisière de 650 à 1100 km/h. Altitude de 30 à 60 m. Charge militaire : 450 à 900 kg. Portée de tir : quelques centaines de kilomètres. Portée d'intervention : 2 000 km (avion).

Le missile balistique (du type Scud)

Charge militaire : quelques centaines de kilos. Portée : 200/300 km.

Avantages : la portée.

Inconvénients : le prix. De plus, il s'avère facilement détectable en vol par les stations radars, vulnérable aux missiles sol-air et air-air, et imprécis (à plus ou moins 100 mètres près, au mieux).

CHAPITRE 2

L'ACHAT D'ARMES

Pour se procurer des armes en grande quantité, il existe un procédé parfaitement rodé qui fait ses preuves depuis des décennies : le détournement de "end-user certificate". Un "end-user" est un document officiel dans lequel un État, lorsqu'il achète des armes, s'engage à ne les utiliser que pour ses propres forces armées et à ne pas les rétrocéder à un pays tiers.

Dans la pratique, la plupart des pays et des industriels s'intéressent peu au devenir des armes et des munitions qu'ils ont vendues, car ils exigent toujours des acheteurs un "end-user certificate" pour se couvrir par rapport à leur propre autorité.

Les différentes procédures pour se procurer des armes

Lorsqu'un pays est en guerre et soumis à un embargo militaire, il s'adresse tout d'abord à un intermédiaire indépendant, le marchand d'armes. En professionnel compétent, celui-ci examine la liste des commissions, dressant la liste des pays producteurs pour chaque type de matériel.

Ensuite, il lui faut trouver un pays qui a déjà acheté ce type de matériel, où la corruption est possible. Ce qui ne manque pas !

L'intermédiaire approche alors un membre bien placé de l'état-major de ce pays et lui verse une grosse commission (qui provient du pays acheteur). En échange, le militaire de haut rang fournit un end-user prouvant que son pays souhaite renouveler ses stocks.

Une fois ce document en main, l'intermédiaire se présente auprès du responsable commercial de la société qui produit le matériel, lui remet le end-user, puis effectue un premier versement à travers des comptes situés dans des paradis fiscaux (procédé largement en usage lors des ventes d'armes). La société livre ensuite le matériel qui est transporté par avion cargo ou bateau vers le pays indiqué sur l'end-user. L'intermédiaire n'a plus qu'à rembarquer le matériel à destination de son client.

Tout les types d'armes peuvent ainsi être achetés, avec cependant une restriction de poids : la taille du matériel. Plus ce dernier est volumineux, plus son déplacement est visible et attire l'attention.

Les chars, par exemple, sont des armes chères et volumineuses, il est donc difficile d'en faire commerce. Le poids d'un char équivaut à celui de plusieurs milliers de roquettes antichars, plusieurs centaines de missiles antiaériens, ou plusieurs dizaines de bombes de 900 kg guidées par laser. De même, les avions de combat passent difficilement inaperçus car la commande doit être adressée non pas à un industriel, mais à une dizaine : le fabricant de l'avion proprement dit, et ceux du moteur, des équipements électroniques et des missiles emportés…

En général, plus l'affaire se maintient sur un plan strictement commercial (et non politique), plus les marchands d'armes apprécient.

Acheter des armes sans les payer

Une astuce également très prisée par les États est de se procurer des armes presque… gratuitement.

Le circuit est un peu plus complexe que pour la vente d'armes traditionnelle, même si le principe reste identique. La différence majeure réside dans le choix de l'industriel qui fabrique le matériel : il faut

qu'il soit situé dans une région à fort taux de chômage et qu'il soit économiquement en difficulté.

Dans un premier temps, un pays tiers commande du matériel à cet industriel, mais il ne le paie pas en prétextant des difficultés financières. Puis il revend ces armes à une organisation ou un pays quelconque.

L'industriel, lui, est remboursé par un organisme d'État chargé d'assurer les exportations.

CQFD.

Ce type d'assurance publique existe dans toutes les grandes nations occidentales.

Personne n'est regardant sur le devenir du matériel, car tout le monde y gagne : le client final qui s'est procuré des armes à bon prix ; le pays intermédiaire qui a vendu des armes qu'il n'a pas payées ; l'industriel vendeur qui touche son argent de l'assureur dépendant de l'État; enfin et surtout, l'État occidental, à travers l'assureur, qui apporte des subventions à un industriel et à une région en difficulté, sans s'attirer les foudres des commissions internationales veillant au respect des règles du libre échange, et s'opposant donc aux subventions d'État.

Le meilleur marché des armes

A notre avis, le meilleur moyen d'obtenir des armes est de se promener dans les pays de l'ancienne Union Soviétique.

Depuis la chute du mur de Berlin, la décomposition de l'ancienne URSS a laissé place à une multitude d'États en difficulté, et qui sont autant de vendeurs potentiels. En outre, ils possèdent des armes de haute technologie, vraiment intéressantes, même si toutes ne sont pas à prendre.

Les terroristes attentionnés se pencheront sur les armes des troupes d'élites de l'armée russe.

Les Spetsnaz sont sélectionnés parmi les meilleurs combattants de la marine russe, tout comme les commandos de la marine française ou les SEALs américains. Ils subissent un entraînement spécial de nageurs de combat et de chuteurs (parachutage à haute altitude à distance de l'objectif). Leurs missions sont la reconnaissance, le sabotage, le minage des voies maritimes et l'élimination de personnalités. Leur nombre oscille actuellement entre trois et quatre mille soldats.

Contrairement à l'infanterie de la marine classique (qui effectue un assaut amphibie à l'aide de péniches de débarquement et d'aéroglisseurs, avec des blindés légers et des véhicules de transport de troupes), les Spetsnaz sont transportés sur le lieu d'intervention par hélicoptère, par parachutage à haute altitude ou par propulseurs sous-marins à deux places.

Ces troupes d'élite sont équipées d'armes conventionnelles, comme les fusils d'assaut AK-74 ou les mitrailleuses RPK-74, et d'autres plus

adaptées à leurs missions, comme des pistolets munis de silencieux ou des fusils sous-marins APS capables de tirer une vingtaine de fléchettes sur une distance de 30 mètres sous l'eau.

Un terroriste peut également s'intéresser à l'une des plus impressionnantes armes russes destinées aux commandos et à l'infanterie : le missile antiaérien tiré à l'épaule.

Le premier missile léger de ce type, le SA-7, apparu en 1966, est en revanche à laisser de côté : trop cher et désuet. Cette arme est néanmoins intéressante, car elle fut utilisée durant la guerre des six jours et surtout la guerre du Yom Kippour par les forces égyptiennes contre les avions israéliens. Bien que léger (9,2 kg), ce petit missile présenta une réelle menace pour la force aérienne israélienne, non pas pour ses performances (sa portée pratique est de 3 à 4 km), mais par le fait que des centaines ou des milliers de soldats peuvent en être équipés et le lancer à tout moment. Les missiles antiaériens plus gros (portée de 6 à 8 km contre les objectifs à basse altitude) sont lancés à partir d'une plate-forme (véhicules blindés, remorques). De plus, le tir de ces missiles est toujours commandé par un radar qui détecte les appareils ennemis. La présence de ce radar et la taille de la plate-forme rendent les sites de lancement de missiles antiaériens relativement visibles pour les appareils de reconnaissance et

d'observation. Ces sites sont donc souvent détruits par des missiles guidés, ou plus simplement contournés.

Une technique utilisée par les Israéliens durant la guerre du Liban en 1982 afin de détecter puis d'anéantir les systèmes de missiles antiaériens consistait à envoyer de petits avions télécommandés (les drones) au-dessus des zones dangereuses. Les Syriens se devaient d'abattre ces engins (dont le coût est inférieur à celui d'un missile), mais dévoilaient ainsi la position de leurs lanceurs de missiles.

Cependant, un missile comme le SA-7 est impossible à repérer. Son emploi s'est donc généralisé. Conséquence : les avions légers d'attaque au sol tels que les appareils de lutte anti-guérilla ont disparu depuis longtemps ; les avions de combat doivent voler au moins à 600 km/h et toujours à très basse altitude (60 mètres), suivant des trajectoires courbes, tandis que les hélicoptères antichars sont réduits au vol tactique qui consiste à croiser en permanence à une altitude de quinze mètres en utilisant tous les masques de terrain.

Pourtant, le SA-7 ne représente plus un grand danger, car son système de guidage à infrarouge, qui suit les sources de chaleur, est facile à leurrer. Si un pilote détecte le lancement d'un missile, il éjecte des leurres infrarouges qui attirent vers eux les SA-7. Les appareils civils de la compagnie El-Al sont munis de

ce type de dispositif.

Depuis la fin des années 70, les SA-7 soviétiques ont toutefois été remplacés par les SA-14. Plus gros (10,5 kg, pour une longueur de 1,4 m et un diamètre de 7 cm), ils sont bien plus performants. Surtout au niveau du système de guidage infrarouge, beaucoup plus sensible et bien plus difficile à leurrer. Le SA-14 est donc à recommander aux terroristes en mal d'armes.

Le SA-16 en est une variante. Dans ce cas, le tireur pointe un faisceau laser vers l'aéronef à abattre et le missile se dirige droit sur la tache du laser.

CHAPITRE 3

FABRICATION D'UNE BOMBE

AVERTISSEMENT

Il NE FAUT SOUS AUCUN PRÉTEXTE TENTER DE METTRE EN PRATIQUE LES INFORMATIONS EXPOSÉES DANS CE CHAPITRE, SOUS PEINE DE S'EXPOSER, ET D'EXPOSER SON ENTOURAGE, À UN DANGER MORTEL. LES FORMULES CHIMIQUES NE SONT DONNÉES QU'À TITRE INDICATIF. ELLES N'ONT PAS ÉTÉ VALIDÉES, ET LES ÉTAPES INTERMÉDIAIRES NE SONT PAS TOUJOURS DÉCRITES. LA FABRICATION, DÉTENTION ET UTILISATION D'EXPLOSIFS SONT FORMELLEMENT INTERDITES PAR LA LOI ET EXPOSENT LES CONTREVENANTS À DE LOURDES SANCTIONS.

Au crépuscule du XXe siècle, les terroristes fabriquent encore des bombes qui datent du siècle dernier.

Cette constatation est surprenante, car les groupes subversifs ont aujourd'hui les moyens de faire beaucoup plus de dégâts. Ils ont la possibilité de fabriquer des bombes perfectionnées, avec des produits publics et pour un prix modique.

La sécurité des États occidentaux dépend donc de la médiocrité des terroristes, de leur incapacité à exploiter les changements de notre société. Cependant, la connerie a des limites. Il est à parier que si un vent de révolution souffle de nouveau dans nos contrées, il emportera tout sur son passage, en particulier nos belles illusions.

Pour fabriquer une bombe, il faut :

– un explosif ;
– un détonateur permettant de le faire exploser ;
– éventuellement un système de guidage pour diriger la bombe vers la cible souhaitée.

Voici les explosifs, détonateurs, guidages que pourraient facilement fabriquer les terroristes pour mener leurs opérations au XXIe siècle.

Les explosifs

L'explosif idéal pour qui ne connaît rien (et ne veut rien connaître) à la chimie est le chlorate de potassium (ClKO3). Lorsqu'il entre en contact avec de l'acide sulfurique, l'explosion est immédiate et très puissante. Le chlorate de potassium est souvent employé en chimie agricole. Son usage est donc assez fréquent. Sa manipulation est cependant délicate, puisqu'il attaque toutes les substances organiques, y compris la peau. Il se présente sous forme de poudre et peut être commandé au prix moyen de 200 F le kilo. Pour 20 000 F, il est possible de se faire livrer la substance sous la forme de deux conteneurs de 50 kg. Il n'y a pas de limitation à son achat.

Plus la quantité d'explosifs est importante, plus les dégâts le sont. Le rayon de destruction d'un explosif est en effet proportionnel à sa masse. Concrètement, il est d'environ quatre fois la racine carrée de la masse d'explosif (pour les explosifs militaires). Pour 100 kg d'explosif, le rayon de destruction sera donc de 40 m.

Par comparaison, un camion rempli d'une tonne d'explosif possède une puissance de destruction équivalente aux plus grosses bombes aériennes. Le pourcentage d'explosif sur la masse totale de la bombe est calculé en fonction de l'action à mener.

Pour une bombe contre le personnel et les véhicules non blindés, ce taux est de 50 %. Pour une bombe de semi-pénétration, contre les objectifs bétonnés, il est de 30 %. Pour une bombe de pénétration, contre la cuirasse des navires, il n'est plus que de 15 %.

Le plus souvent, l'effet destructeur des explosifs d'une bombe est focalisé dans une direction particulière, pour être plus efficace. C'est le cas de tous les missiles antichars.

Pour cela, il faut fabriquer une "charge creuse". Une méthode simple consiste à se munir d'un fond de bouteille de champagne, dont la forme correspond à celle des charges creuses militaires. Les magnums de 1,5 litre permettent de fabriquer des charges creuses de un ou deux kilos, capables de transpercer un mètre de béton armé ou une dizaine de centimètres d'acier. On remplit cette moitié de bouteille d'explosifs que l'on tasse.

Achat des produits chimiques

Pour acheter des produits chimiques, il est préférable de monter une société écran. Et plus particulièrement une société agricole, car la chimie des engrais se rapproche de celle des explosifs.

Les phosphates naturels sont en effet transformés en superphosphates par un mélange avec de l'acide

sulfurique, de l'acide chlorhydrique ou de l'acide phosphorique. Le chlorate de potassium est un désherbant. On retrouve donc dans ce domaine tous les ingrédients utiles à l'élaboration d'explosifs.

De plus, l'industrie des engrais n'est pas une industrie à forte intégration verticale. Autrement dit, jusqu'à la dernière étape, avant la livraison chez l'agriculteur, les engrais sont travaillés et subissent divers traitements. C'est le cas des engrais composés, qui ne sont que des mélanges d'engrais de base (azotés, phosphatés ou dérivés de la potasse). Ils sont élaborés à la demande des agriculteurs régionaux.

Les entreprises d'engrais de petite taille sont naturellement amenées à commander et à manipuler de grosses quantités de produits de base et intermédiaires.

La France produit à elle seule quatre millions de tonnes d'engrais. Les pays de l'Est fournissent tous les ingrédients de base qui sont issus de la chimie lourde, ainsi que les intermédiaires. Rien n'interdit donc d'ouvrir une petite unité de production dans ces pays-là.

Les détonateurs

La maîtrise des détonateurs est plus importante que celle des explosifs. A quoi sert en effet un explosif qui n'explose pas ?

Ce problème est particulièrement aigu pour les militaires. Durant la guerre des Malouines, au début des années 80, près de la moitié des bombes larguées par les avions argentins n'ont pas explosé à cause de la défaillance des détonateurs. Pendant la vague d'attentats qui déferla sur la France en 1995, nombre de vies furent sauvées par les défauts des détonateurs. Ce fut le cas d'une bombe découverte le 26 août 1995 sur le parcours du TGV Paris-Lyon, ou d'une autre, trouvée dans une sanisette parisienne le 4 septembre. Sur celle-ci, le retardateur était une horloge aux aiguilles reliées à un détonateur électrique.

Classique, penseront les amateurs de films policiers. Mais il existe un grand nombre de détonateurs : mécaniques, électriques, thermiques ou même chimiques…

Les détonateurs mécaniques

La méthode la plus simple consiste à employer une de ces fusées d'appel au secours qu'utilisent les marins. Il suffit de relier la gâchette à un fil d'acier, puis de diriger la fusée vers l'intérieur de l'explosif.

Cette technique pour le moins rustique a l'avantage de convenir à un mouvement subversif dont les membres n'ont pas été sélectionnés pour leurs qualités intellectuelles. Dans le cas d'une

explosion au moment du choc, c'est un détonateur à impact à retenir.

Il faut commencer par se procurer des amorces de cartouche (en vente libre chez les armuriers par paquets de cent). On enfonce une amorce dans l'explosif et on place un tube de quelques millimètres de diamètre au-dessus. Du côté de l'amorce, on introduit ensuite une tige métallique munie d'une pointe. Un ruban adhésif permet de la maintenir à quelques millimètres de l'amorce.

En cas de choc violent, la tige s'enfonce dans le tube et la pointe déclenche l'amorce avant l'explosion. Ce système est particulièrement utile pour armer une bombe placée dans un ULM ou une voiture en mouvement.

Les détonateurs électriques

Les détonateurs électriques comptent parmi les plus efficaces qui soient, car ils se déclenchent à volonté et à distance. Il est également facile de relier les fils à une télécommande ou à des capteurs de détection. Paradoxalement, ce type de détonateur est en vente libre dans de nombreux pays pour quelques francs. Il s'agit des déclencheurs de ces petites fusées que lancent les enfants dans le cadre de clubs de découverte. On trouve aussi ce type de produit dans les magasins de modélisme.

La plupart du temps, les détonateurs électriques sont utilisés pour faire exploser des voitures piégées. Dans ce cas, le déclencheur est une simple batterie. Sur le même principe, il est facile de réaliser un interrupteur qui se déclenche lorsque l'on déplace la bombe. Il faut prendre une ampoule de quelques centilitres, type ampoule médicale. Une fois les deux bouts ouverts, on y introduit l'équivalent d'un dé à coudre de mercure. Puis, à chaque extrémité, un fil électrique dénudé est enfoncé à l'intérieur de l'ampoule. L'étanchéité est obtenue à l'aide de mastic.

Le mercure est un métal liquide conducteur d'électricité. Le moindre mouvement fait circuler le liquide. Si le mercure s'étale sur toute la surface, il relie les deux fils et le courant passe, alimentant et déclenchant le détonateur électrique.

Le retardateur électrique le plus usuel est l'horloge. Une aiguille recouverte de cuivre ou de papier aluminium est reliée à un fil électrique. Lorsque l'aiguille rencontre un fil dénudé fixé à l'horloge par un bout de ruban adhésif, le courant passe et déclenche l'explosion. Cette technique représente toutefois le meilleur moyen de rater un déclenchement. En effet, l'introduction d'un mécanisme délicat dans un système le rend encore plus fragile. De plus, des problèmes de fiabilité dus à la chimie et à l'électricité viennent se greffer sur les

difficultés mécaniques. A force de multiplier les étapes, la fiabilité est fortement réduite. Enfin, le chlorate de potassium ne peut être déclenché par un tel détonateur.

Le détonateur thermique

Derrière ce terme technique se cache la plupart du temps… une banale cigarette. En effet, la chaleur dégagée par une cigarette embrase des allumettes, puis un liquide incendiaire qui déclenche l'explosion. Mais la durée de vie d'une cigarette est comprise entre 5 et 10 minutes. C'est tout juste suffisant pour se mettre à l'abri.

Et pour transformer une cigarette en détonateur, il faut également s'assurer de sa stabilité. Une astuce simple consiste à enfoncer des fils d'acier à l'intérieur afin de la rigidifier.

Le détonateur chimique

La détonateur chimique est le détonateur par excellence pour déclencher une explosion. Il consiste à mettre en présence de l'acide sulfurique et du chlorate de potassium (ou du permanganate de potassium). On place l'acide sulfurique dans une fiole de verre qui est entourée de chlorate de potassium. Lorsque le verre se brise, l'explosion se

produit. De tous les types de détonateur, le chimique est le plus simple et le plus efficace. Une fois que la réaction commence, rien ne peut l'arrêter. À ce titre, la fiabilité est excellente. D'ailleurs, pendant la deuxième guerre mondiale, les Allemands les appréciaient particulièrement. Pour l'attentat raté (mais pas à cause du détonateur) contre Hitler, c'est cette solution qui fut retenue.

La principale difficulté consiste à réaliser un retardateur chimique. Pour cela, on place entre l'acide sulfurique et le chlorate de potassium une feuille (épaisse) d'aluminium. L'acide sulfurique ronge peu à peu l'aluminium (en jouant sur l'épaisseur, on module le retard). Pour que cela fonctionne, il ne faut pas que l'acide soit dans un conteneur d'aluminium hermétique. En effet, la réaction de l'acide sulfurique et de l'aluminium dégage de l'hydrogène. Le conteneur peut être endommagé sous la pression de l'hydrogène gazeux. Il faut donc prévoir un orifice d'évacuation du gaz.

Deux bombes intéressantes

Une bombe-appartement

La transformation d'un appartement (ou d'une maison) en bombe est particulièrement intéressante pour assurer sa fuite lors d'une attaque de l'ennemi

ou pour détruire un bâtiment.

Une méthode rudimentaire consiste à remplir 10 % d'un lieu clos (un appartement, par exemple) avec du méthane. Attention : si la dose dépasse cette valeur de plus de 5 %, le mélange n'est plus explosif. Le dosage doit donc être précis.

Pour déclencher l'explosion à distance, le plus efficace consiste à utiliser un briquet piézo-électrique (usuellement employé par les ménagères pour allumer les cuisinières au gaz). Un petit montage "électronique amusant" permet de le munir d'un interrupteur commandable à distance. Dans une version plus sophistiquée, il est possible de commander l'interrupteur via le téléphone. Dans ce cas, l'explosion peut être déclenchée à plusieurs milliers de kilomètres.

Une bombe aéroportée

Une bombe aéroportée est particulièrement difficile à réaliser. Mais voici une méthode simple pour en fabriquer une.

Il faut tout d'abord se procurer un obus désamorcé pour collectionneur : calibre 105 mm, 155 mm ou 203 mm (ce sont des calibres de l'OTAN). Ensuite, commander un tube d'acier sans soudure de même diamètre interne que l'obus désamorcé. Puis, fermer une extrémité en soudant l'obus désamorcé et le tube

d'acier. Souder des empennages d'environ dix centimètres de large à l'autre extrémité. Refroidir le tube à l'aide d'un tuyau d'arrosage dans lequel circule de l'eau froide. Remplir le tube d'explosif puis bien tasser (l'explosif s'échauffe lorsqu'il est tassé, c'est pourquoi il faut bien veiller à ce que le circuit de refroidissement fonctionne). La mise en place du détonateur nécessite de placer quelques litres d'acide sulfurique pur dans une bouteille en verre. Insérer une plaque d'aluminium, dont l'épaisseur est déterminée par des tests, entre la bouteille d'acide sulfurique et l'explosif.

Le guidage des bombes et des missiles

Durant la guerre des Malouines en 1982, la quasi-totalité des actions offensives argentines furent menées par l'aviation, à savoir 75 chasseurs Skyhawk, 45 Mirages III ou Dagger (clone israélien du Mirage) et 5 Super-Étendard (avec des missiles Exocet), soit en tout 125 avions d'attaque.

Mise à part les Super-Étendard, tous ces appareils larguaient des bombes au-dessus de leur objectif après un léger piqué. Aucun équipement sophistiqué de navigation ou de guidage ne fut utilisé. Or, plus de la moitié des bombes larguées n'explosèrent pas (défaut de détonateurs). Un grand nombre d'avions furent également abattus avant de lâcher leurs

bombes, car en s'approchant à quelques dizaines de mètres des cibles, les appareils s'exposaient à l'artillerie anti-aérienne et aux missiles des navires.

La guerre des Malouines rappelle à cet égard la deuxième guerre mondiale, pendant laquelle des moyens énormes furent employés pour un rendement négligeable.

Par exemple, l'attaque d'une usine d'eau lourde en Norvège mobilisa pas moins de 158 bombardiers qui larguèrent 1 250 bombes. Seules 4 bombes atteignirent leur objectif, soit un rendement de 0,3 %. Il faut donc un système de guidage pour optimiser les attaques stratégiques et limiter les pertes au maximum.

Si, pour la guerre des Malouines, les bombes avaient été larguées à distance de sécurité (8 à 12 km à basse altitude), les pertes auraient été divisées par quatre.

Et si, pendant la deuxième guerre mondiale, on avait placé un système de guidage terminal sur les bombes, on aurait multiplié par cent l'efficacité des opérations.

Aujourd'hui, les terroristes ont les moyens de fabriquer ou de se procurer à bas prix des systèmes de guidage. Ils pourraient les utiliser par exemple pour transformer un avion, un ULM, ou un bateau… en missile.

Les systèmes de guidage

Il faut différencier les systèmes de guidage terminal des systèmes de navigation. La différence essentielle réside dans la précision. Pour la navigation, il suffit de connaître sa position, à intervalles réguliers, avec une précision comprise entre quelques dizaines et centaines de mètres. Les systèmes de guidage terminal possèdent une précision de quelques mètres ; ils sont donc 10 à 100 fois plus précis que les systèmes de navigation.

Pour guider une bombe ou un missile, on utilise un système de navigation pendant les premières phases du trajet ; dans la dernière phase, un système de guidage prend le relais, soit à une distance de un ou deux kilomètres de la cible.

Les systèmes de navigation

Il existe grosso modo quatre systèmes de navigation : la centrale inertielle, le système GPS, le radar de suivi de terrain et le système Tercom.

La centrale inertielle a l'avantage d'être un système autonome et n'a besoin d'aucune référence extérieure (elle indique la position par inertie des gyroscopes qui conservent leur position initiale malgré les mouvements de l'appareil).

Les centrales inertielles à fibre optique sont les

plus économiques, car elles ne contiennent aucune partie mobile ni gaz. Néanmoins, ce sont des systèmes délicats à fabriquer. Ils sont technologiquement ardus à élaborer à cause des contraintes optiques et mécaniques. Leur coût est également élevé (plusieurs millions de francs pour le haut de gamme).

Le système de repérage par satellite GPS (Global Positionning System) a l'avantage d'être précis (50 m), bon marché (1 000 F), léger (quelques centaines de grammes), et de s'interfacer naturellement à un ordinateur portable. L'inconvénient est qu'il dépend du réseau de satellites GPS de l'armée américaine, qui peut décider à tout moment d'éteindre les satellites et de rendre le système inopérant.

Le radar de suivi de terrain, en revanche, a l'avantage d'éviter les obstacles qui se présentent devant l'appareil, surtout à basse altitude. Il est néanmoins très cher, et impossible à se procurer pour un civil. Enfin, l'émission radar est détectable à plus d'une centaine de kilomètres par des avions de surveillance.

Le système Tercom de suivi de terrain (utilisant un altimètre radar, laser ou barométrique) permet un vol à basse altitude sans radar (guidage par repérage des obstacles naturels). Il est cependant inutilisable sur de grandes étendues de plaine, de désert ou de mer.

Conclusion : le GPS est le système de navigation le plus performant et le plus économique.

Il est également possible de compléter les informations issues des satellites en orbite par des émetteurs placés au sol pour en faire un système de guidage terminal. Dans ce cas, la précision du GPS est d'environ trois à cinq mètres.

Les systèmes de guidage terminal

Il existe trois sortes de guidage terminal : les systèmes de désignation par laser, les systèmes de guidage par radar et les caméras vidéo de vision à distance.

Les systèmes à guidage par laser (ou par faisceau hyperfréquence) sont apparus durant la guerre du Vietnam. Mais ce n'est que pendant la guerre du Golfe qu'ils ont été utilisés à grande échelle.

Le principe est simple : un observateur au sol ou dans un appareil d'observation est muni d'un laser CO2 (émission dans l'IR). Il pointe le faisceau vers la cible et la tache du laser désigne celle-ci. Le missile est équipé de plusieurs détecteurs qui ne sont sensibles qu'à la fréquence du laser. Le missile se "centre" sur la tache laser et l'atteint avec une précision de quelques mètres. Ces systèmes ont l'avantage d'être précis (quelques mètres), peu coûteux (cent fois moins qu'un système de guidage

par radar) et difficiles à brouiller. Néanmoins, ils nécessitent la présence d'un désignateur à quelques kilomètres de la cible (soldat au sol, dans un véhicule, un avion, un hélicoptère).

Les systèmes de guidage par radar sont de loin les plus sophistiqués ; paradoxalement, ce sont aussi les moins efficaces. Ils équipent les missiles anti-navires (Exocet) et un missile nucléaire tactique américain, le Pershing II. À quelques kilomètres de l'objectif, le radar placé dans le nez de l'appareil se met en route et donne une image (radar) du terrain, permettant de situer la cible dans son environnement. Très peu de missiles sont équipés de ce type de système de guidage, cher et relativement facile à brouiller. La qualité des images est mauvaise (le plus petit détail visible sur une image radar mesure 3 mètres de côté). Le radar est aussi difficile à exploiter à cause des leurres utilisés pour défendre la cible.

L'ordinateur de bord du missile éprouve enfin de grandes difficultés pour interpréter les images. L'ordinateur met en effet en œuvre des logiciels de reconnaissance des formes qui ne sont pas encore au point. Dès que l'image est un peu brouillée ou que des parasites apparaissent, la reconnaissance de la cible devient aléatoire. Dans un environnement difficile (comme dans le cas où la cible est un navire muni d'un système de brouillage électronique des radars), l'efficacité du système de guidage par radar

est presque nulle. Il a cependant quelques avantages : le guidage est automatique sans désignation de cible, et il fonctionne par tous les temps.

Les caméras vidéo de vision à distance montées dans le nez d'un appareil ont l'avantage d'être peu onéreuses (plus que le guidage par laser, mais bien moins que le guidage par radar). Elles sont précises et ne nécessitent pas la présence d'un désignateur à proximité de la cible. Elles restent néanmoins difficile à télépiloter à travers un système de vision à distance, étant donné la vitesse de déplacement de l'engin. Et elles ne fonctionnent pas par mauvais temps

Conclusion : le meilleur système de guidage terminal est la désignation de cible par laser ou faisceau hyperfréquence. Beaucoup plus précis, plus économique et plus fiable que le guidage par radar.

Fabrication d'un système de guidage terminal par laser

La fabrication d'un système de guidage par laser par un petit groupe de techniciens n'est pas irréaliste. En revanche, sa mise en œuvre s'avère beaucoup plus délicate.

Durant la guerre des Malouines, les forces britanniques eurent le plus grand mal à utiliser les bombes guidées par laser (lasers Paveway, réalisés

par Texas Instruments). Ces armes étaient montées sur des avions (Harrier) à décollage vertical, basées sur les porte-avions de la Royal Navy. Les bombes étaient larguées suivant une trajectoire balistique par un premier Harrier, pendant qu'un second illuminait la cible à l'aide de son laser de bord. À la grande surprise des pilotes, les bombes s'écrasèrent au sol bien avant d'atteindre leur objectif. La raison était fort simple : les lasers avaient été allumés beaucoup trop tôt.

Pour construire un tel système, il faut grosso modo réaliser un désignateur, des détecteurs et un circuit électronique qui compare les signaux des détecteurs. Pour la partie désignateur, il faut un laser CO2 de quelques watts de puissance et un petit télescope IR utilisé pour focaliser le faisceau du laser sur une grande distance. La partie à monter sur le missile se composera de quelques détecteurs (3 ou 5) placés en bouquet à l'avant de l'appareil. Un circuit électronique relativement facile à réaliser compare les signaux issus de trois détecteurs. Si l'intensité du signal issu d'un des détecteurs est supérieure aux autres, le dispositif électronique manœuvre les commandes de vol de manière à ce que le missile corrige sa position et que les trois détecteurs délivrent le même signal. Dans ce cas, cela signifie que le missile est aligné sur la tache laser, donc sur la cible.

Tous ces composants, sans restriction, sont

disponibles chez les fournisseurs de matériel optique pour laboratoires.

Pour les acheter, il suffit de se présenter via une entreprise de recherche. Il existe en Europe des centaines de petites sociétés de moins de 10 personnes qui effectuent des recherches pour les grands groupes industriels. Il n'y a donc rien d'anormal à vouloir acquérir ce type de matériel.

Utilisation du système GPS (Global Positionning System) de navigation par satellites

L'ancêtre du GPS fut dans les années 60 le programme TRANSIT de radionavigation par satellite, destiné à guider des missiles à tête thermonucléaire (Polaris) tirés par les sous-marins américains. Les progrès de l'électronique aidant, la radionavigation par satellite devint d'un intérêt croissant et, en 1973, le programme GPS fut lancé.

Mais comment un système militaire stratégique a-t-il put se retrouver dans les rayons des supermarchés ?

La raison réside dans la catastrophe du 747 de la Korean Airlines, abattu au-dessus du territoire soviétique le 31 août 1983, coûtant la vie à 269 civils. L'avion avait en effet dévié de 700 km de sa route à cause d'une défaillance du système de navigation inertielle et de radionavigation à partir des stations terrestres. Le président Reagan déclara que le GPS

serait dorénavant disponible pour les civils. Pour éviter que ses adversaires l'utilisent à des fins militaires, le département de la défense américain introduisit volontairement une perturbation dans le signal émis par les 24 satellites. L'effet de cette perturbation restreint la précision du système civil à 100 mètres. Seuls les récepteurs militaires possèdent une électronique qui compense la dégradation du signal et retrouve la précision initiale.

Néanmoins, les utilisateurs civils lancèrent le DGPS, bien plus précis que le GPS civil. Plus de 4 000 aéroports et terrains d'aviation US l'ont ainsi adopté pour aider à la navigation et à l'approche finale des avions civils. Les groupes subversifs peuvent donc très bien aujourd'hui utiliser un système DGPS pour guider des bombes ou autres appareils volants. D'ailleurs, l'armée américaine envisage depuis une décennie de se retrouver devant un ennemi utilisant son propre système GPS contre elle.

Selon l'analyste Irving Lachow, de la RAND Corporation, le Pentagone et les services secrets américains comptent sur la facilité à repérer les sites DGPS au sol, pour les brouiller ou les détruire.

Il est probable que les avions de reconnaissance électronique, qui scrutent les fréquences hertziennes, sont munis de programmes informatiques spécifiques pour localiser les stations GPS et en fournir une liste exhaustive. Mais, qui sait…

PARTIE 4

LES VRAIES ET FAUSSES CIBLES DES TERRORISTES

CHAPITRE 1

LES CIBLES CIVILES

Pour optimiser une action de déstabilisation, on doit rechercher le meilleur rapport entre l'opération à mener et le résultat souhaité. Les cibles de choix sont donc des lieux dont la destruction engendre un maximum de dégâts, si possible pour un minimum de sueur.

Dans ce cadre, les usines chimiques, les centres de production d'énergie, les centres bancaires stratégiques, les services de renseignement de la Police sont des cibles idéales. À l'inverse, la plupart des entreprises, des administrations, des banques… ne sont aujourd'hui plus que des bureaux. Il est donc absurde de les attaquer.

Il en va de même pour les usines, qui sont nombreuses à faire la même chose et ne sont pour la plupart que des salles d'assemblage. Exemple, les usines de conditionnement et d'emballage, qui se comptent par milliers, ne présentent aucun intérêt stratégique.

Les vraies cibles civiles

Les usines chimiques

Les grandes usines de la chimie de base comme les petites de la chimie fine sont des cibles de choix. Les terroristes choisiront une installation chimique plutôt qu'une autre selon deux critères :

- la position de l'usine et le sens des courants aériens environnants ;
- le type de produit chimique fabriqué.

Pour satisfaire au premier critère, il existe une liste des installations chimiques mondiales. Il s'agit de deux bases de données, Chemical Age Project File et Chemical Plant Database, consultables par abonnement et régulièrement remises à jour.

Pour le deuxième, de nombreux ouvrages et bases de données décrivent les caractéristiques et surtout la toxicologie de dizaines de milliers de produits chimiques commercialisés à travers le monde.

Chemical Toxicology of Commercial Products recense 23 000 produits chimiques commerciaux et décrit toutes leurs caractéristiques toxicologiques. En France, les fiches toxicologiques de l'Institut National de Recherche et de Sécurité sont en vente libre.

Enfin, pour suivre à la trace le flux des produits chimiques, il suffit de se référer à l'ouvrage Chemical Economics Handbook (Éditions SRI International), qui établit des listes d'achats et de ventes. À connaître si l'on prévoit une attaque lors du transport des produits.

L'industrie du gaz naturel

La filière du gaz naturel constitue une cible parfaite pour un maximum de dégâts irréversibles avec un minimum de moyens. Son infrastructure est en effet sensible, à cause de la concentration physique des investissements et des technologies sur une surface donnée (usine de liquéfaction, méthanier, centrale électrique à turbine au gaz).

Une usine de liquéfaction coûte plus d'un milliard de dollars. Il est inutile d'y pénétrer (elle s'étend sur plusieurs hectares) pour la détruire. Il suffit de déclencher un bombardement à l'aide d'une demi-douzaine de mortiers, à quelques kilomètres de distance, durant une période de 20 à 30 minutes. La

taille de l'usine, son prix et sa vulnérabilité aux explosifs en font une cible idéale.

Ce raisonnement est également valable pour les méthaniers, particulièrement vulnérables lors des opérations de chargement et déchargement dans les ports.

Les centrales à turbine au gaz sont aussi vulnérables, une turbine de quelques tonnes et dizaines de mètres de long constituant le cœur et la pièce maîtresse de l'infrastructure. Cette turbine est directement reliée à une centrale électrique.

La réserve fédérale américaine : une cible de choix

Comme nous l'avons déjà précisé (cf. "Le financement des groupes terroristes"), s'attaquer au marché financier n'est pas une bonne stratégie. Il est absurde de s'aliéner un moyen de financement important.

Néanmoins, dans le cas d'une action de détérioration pure, la Réserve Fédérale Américaine (RFA) est une cible de choix s'il s'agit de paralyser l'ensemble du réseau bancaire mondial.

Créée en 1913 par le congrès, la RFA est à la fois le gendarme des banques américaines et le décideur du volume d'argent liquide en circulation. Elle effectue chaque jour 1 250 milliards de dollars de

transactions, soit 50 milliards de dollars transférés chaque heure. Sa paralysie entraînerait celle de tout le système bancaire américain et par voie de conséquence, un arrêt de fonctionnement du réseau bancaire mondial. Mais comment paralyser cet organisme ?

Un moyen simple : pour ses transactions, la RFA utilise un réseau informatique spécialisé, dénommé FEDNET, mis en place pour relier tous les centres bancaires.

Depuis quelques décennies, les transactions bancaires ne se font plus par déplacement physique d'argent mais par des ordres de transferts de fond, c'est-à-dire par des échanges de fichiers informatiques à travers ce réseau.

C'est une société privée de service informatique, Ascom Timeplex, qui a réalisé FEDNET et en assure le service après-vente, c'est-à-dire le dépannage en cas de problèmes sur le réseau. FEDNET possède des liaisons à haut débit entre les six principaux sites : Chicago, Saint-Louis, Dallas, Eroc, Richmond et Kansas City. Les autres sites et des milliers de banques clientes sont reliés à ce réseau central.

La destruction de toutes ces lignes de communication (y compris les liaisons de secours par satellites) immobiliserait en quelques jours près de la moitié de l'activité bancaire des États-Unis. Concrètement, si le FEDNET est endommagé, les

banques commerciales ne peuvent plus entreprendre d'actions de compensation, comme encaisser un chèque ou effectuer un virement.

Les services de renseignement policiers

Le pouvoir des services de police, de contre-espionnage et de renseignements réside dans deux fichiers informatiques :

– le fichier des appels téléphoniques ;
– le fichier de toutes les opérations bancaires (FICOBA en France et PROMIS aux USA). Il recense tous les comptes et mouvements bancaires, que les banques sont tenues de transmettre aux banques centrales. Ce fichier est consultable par les agents du fisc.

Ces deux outils de surveillance sont de loin les plus efficaces pour contrecarrer les actions terroristes. En remontant sur plusieurs années, on retrouve toutes les actions, tous les contacts et plus généralement le parcours de toute personne.

Les États-Unis disposent à cet égard d'un avantage important, car les seules cartes de crédit utilisables à l'étranger sont Visa et Mastercard. Or ces deux réseaux bancaires sont américains, et toutes les opérations du monde sont validées en temps réel

par les États-Unis, en particulier par la CIA. L'attaque des services qui gèrent et sauvegardent ces logiciels serait bien sûr stratégique.

Pour se prémunir contre une mauvaise surprise, les terroristes ont intérêt à n'utiliser que des cabines publiques et à payer en liquide. Les filatures, les écoutes et autres méthodes policières sont des opérations peu rentables, car il faut déployer de grands moyens humains et financiers pour obtenir des renseignements utiles.

Par exemple, pour une surveillance continue 24 heures sur 24 comme en pratiquent la police et les services des douanes, il faut mobiliser en permanence 12 personnes, plusieurs véhicules (voitures et motos), voire un hélicoptère (en dehors des centres urbains). Cette dépense de moyens peut être aisément mise en difficulté si l'on suit certaines règles simples de prudence comme enchaîner les modes de transport ou utiliser des immeubles munis de plusieurs sorties. Quant à la mise sur écoute, elle nécessite d'avoir déjà repéré un individu et d'analyser en détail tous les enregistrements.

Rien n'empêche deux personnes d'échanger des informations en toute confidentialité, si elles utilisent la messagerie électronique d'Internet (le e-mail) avec un logiciel de cryptographie.

Les fausses cibles civiles

Le réseau téléphonique : une cible séduisante… mais une fausse cible

Le réseau téléphonique est une cible séduisante. En effet, une soixantaine de centres principaux contrôlent toute la France. Ces centres semblent donc des cibles privilégiées pour paralyser le pays.

En fait, rien de plus faux. Les réseaux téléphoniques sont architecturés en pyramide. Au niveau le plus bas se trouve le réseau local : les commutateurs, qui regroupent des milliers de lignes de téléphone chacun. Ils communiquent avec les commutateurs voisins à l'aide de lignes à 155 Mo/s (l'équivalent de 2 500 lignes à 64 Ko/s), c'est-à-dire ayant une capacité de 2 500 conversations simultanées. Il existe 6 000 centres locaux de rattachement (CLR), qui relient 30 millions d'abonnés. Si l'on veut joindre une personne située à une centaine de kilomètres, la communication passe par un niveau supérieur. Ce sont les 1 500 Centres à Autonomie d'Acheminement (CAA) reliés entre eux par des lignes à 600 Mo/s.

Enfin, au niveau supérieur se trouve le réseau national, permettant les communications longue distance (au-delà de quelques centaines de kilomètres). À ce niveau, il n'existe qu'une soixantaine de commutateurs, reliés entre eux par un

réseau de fibres optiques à 2,5 Go/s (soit l'équivalent de 40 000 communications à la fois). Ces commutateurs se répartissent entre une cinquantaine de Centres de Transit Secondaire (CTS) et une dizaine de Centres de Transit Régional (CTR)

Or, la destruction des centres principaux n'entraîne pas l'arrêt des centres locaux. Les CTS et CTR sont en effet autonomes des CLR et CAA. La destruction des 60 centres principaux interdirait les communications longue distance, mais pas les appels locaux et régionaux.

CHAPITRE 2

LES CIBLES MILITAIRES

Les cibles stratégiques sont les forces nécessaires d'un arsenal militaire.

À l'heure actuelle, la suprématie militaire d'un État, en particulier des États-Unis, repose sur les opérations suivantes :

– la détection et localisation parfaite des radars ennemis, à l'aide d'un système de reconnaissance électronique aérien. Les Américains utilisent pour cela les fameux AWACs, ces avions de surveillance équipés d'un disque-radar ;
– la localisation des mouvements terrestres ennemis, à l'aide des radars MTI ;

– l'identification de toutes les sources radio (radars, communications) provenant de l'ennemi à l'aide d'un système de reconnaissance électronique passive ;
– la neutralisation des défenses aériennes, des radars et missiles. Les avions de brouillage s'occupent de l'électronique des radars, les satellites Infrarouge détectent les tirs de missiles, et les avions télécommandés leurrent les missiles ;
– la destruction des cibles des radars par le largage de missiles antiradars et de bombes (type "clusters"), des avions ennemis par le tir à distance de missiles air-air moyenne portée avant qu'ils n'atteignent leur régime de croisière.

Ces procédures furent suivies par l'armée américaine lors de la guerre du Golfe, et par l'armée israélienne pour le nettoyage des sites de missiles syriens des plaines de Bekaa en 1982.

L'opération Désert Storm, en Irak, en est un bon exemple, car elle eut lieu à grande échelle et le résultat fut net et sans bavure. Il y eut 110 000 sorties d'avions. Les frappes aériennes durèrent 38 jours sans interruption. Sous la direction des AWACs, 300 avions alliés furent utilisés vingt-quatre heures sur vingt-quatre. Les Alliés détectèrent ainsi

500 radars répartis sur 100 sites ennemis. Toutes les cibles terrestres furent détruites. Sur les 724 avions irakiens, seuls 121 réussirent à se réfugier en Iran hors des zones de combat ; 33 autres décollèrent, mais furent détruits en combat aérien. Pour les 570 avions restants, à peine décollèrent-ils de leur base qu'ils étaient repérés par les AWACS et pris en chasse par les intercepteurs (F 15 C) à l'aide de missiles à moyenne portée.

À ces forces militaires, il faut ajouter les très gros hélicoptères qui permettent de déposer une quarantaine de soldats à quelques kilomètres de leur cible, en zone ennemie, ainsi que les gros avions de transport qui assurent la logistique, opération clé des conflits armés.

En conclusion, les terroristes qui voudront amoindrir les forces d'un pays s'attaqueront en priorité aux radars aéroportés sur les AWACs, les avions radars MTI et les satellites Infrarouge.

En second lieu, ils feront peser leurs efforts sur :

– les avions de transport lourds, afin de casser la capacité logistique ;
– les avions d'attaque, ou plus exactement les bases aériennes ;
– les très gros hélicoptères utilisés pour transporter des commandos.

Les vraies cibles militaires : les moyens de surveillance militaire des objets mobiles

Les radars aéroportés

La menace, pour une organisation subversive qui emploie des ULM, planeurs, missiles, avions… réside dans les radars aéroportés. Ces radars sont les seuls outils qui localisent et identifient les objets mobiles. Ni les satellites de reconnaissance, ni les moyens d'observation optique (télescope IR ou classique) n'offrent les mêmes possibilités.

Les radars aéroportés sont donc des cibles prioritaires pour toute action subversive. Car les moyens de localisation des objets mobiles sont les outils stratégiques de gestion des opérations militaires.

Il existe quatre types de radars aéroportés réellement efficaces :

– les AWACs, pour la détection les avions en vol, les hélicoptères et les bateaux ;
– les radars MTI, pour la localisation des véhicules terrestres en mouvement ;
– les satellites infrarouges, pour la détection de tirs de missiles ;
– la reconnaissance électronique passive, qui permet d'identifier toutes les sources radio (radars et systèmes de communication).

Pour bien comprendre pourquoi les AWACs et les radars MTI sont essentiels, il faut se reporter aux informations que délivrent les autres moyens d'observation. Quel que soit leur mode de fonctionnement (IR, visible, radar…), les autres engins sont des appareils de télédétection, c'est-à-dire que les informations qu'ils délivrent concernent la totalité des zones observées. Plus les appareils sont précis, plus la quantité d'informations à analyser est grande. Les informations pertinentes sont alors noyées dans un océan de données. Le travail d'analyse devient presque insurmontable.

Pour repérer un véhicule terrestre, par exemple, il faut passer au peigne fin toute la surface observée, soit des dizaines de millions de points. En revanche, avec un radar MTI, seuls les appareils en mouvement apparaissent à l'écran, donc au plus quelques centaines.

Les AWACs

Ce sont plus exactement les 68 quadriréacteurs E-3F Sentry (34 pour l'US Air Force, 18 pour l'OTAN, 5 pour l'Arabie Saoudite, 7 pour la Grande-Bretagne et 4 pour la France à la 36e Escadre de détection aéroportée d'Avord dans le Cher) et les biturbopropulseurs E-2C Hawkeye (dont près de 150 pour l'US Navy, 4 pour Israël, 6 pour l'Egypte, 12

pour le Japon et 4 pour Singapour), plutôt destinés à la surveillance au-dessus de la mer.

Les radars MTI

Les radars MTI (Moving Target Indication) ne détectent que les véhicules terrestres (ou proches du sol, comme les hélicoptères) dont la vitesse est supérieure à quelques kilomètres par heure. Ils intègrent la position des véhicules, leur vitesse et leur type (voiture, camion, véhicule blindé ou hélicoptère à très basse altitude).

Le système le plus performant au monde est actuellement intégré à l'avion E-8C, construit sous la maîtrise d'œuvre de Northrop Grumman dans le cadre du programme Joint STARS (Joint Surveillance Target Attack Radar System).

Cet avion est, comme l'AWAC E-3 Sentry, un Boeing 707 quadriréacteur civil modifié pour emporter un radar. Contrairement à son confrère, il n'est pas surmonté d'un disque. Le radar se trouve dans une protubérance située sous le nez de l'avion. L'antenne travaille dans la bande de fréquence I (8 à 12 GHz). Sa portée de détection au sol est de l'ordre de 200 km, voire 300 km si les conditions topographiques du terrain sont optimales. Cette longue portée résulte de l'altitude de vol de l'avion, qui est de 12 000 m. Le E-8C peut ainsi se tenir à

200 km de la zone observée.

Ce n'est qu'au début des années 90 que ces avions ont été livrés à l'armée américaine. Pourtant, lors de la guerre du Golfe, des prototypes ont été opérationnels au-dessus du Koweït. Selon des sources officieuses, les informations obtenues par les E-8 ont été cruciales pour l'état-major américain, au point que la mise en service des appareils en fut accélérée. Le commandement américain aurait estimé que la valeur militaire des données délivrées par le radar MTI dépassait de beaucoup celles des satellites.

Le programme Joint STARS ne se résume pas aux E-8. Il comprend un système de communication numérique complexe permettant de diffuser les données en temps réel vers des stations de traitement au sol. Les E-8C servent ainsi de centre de commandement opérationnel. L'appareil, qui pèse plus de 150 tonnes, emporte 70 tonnes de carburant. Il peut tenir en l'air durant onze heures, voire vingt avec un ravitaillement en vol. Les limites sont alors imposées par les membres de l'équipage. Deux équipes de trois pilotes se relayent, et vingt-huit opérateurs surveillent les écrans. En tout, l'armée américaine dispose de dix à vingt E-8C.

La France possède un dispositif semblable mais plus modeste, l'Horizon (Hélicoptère d'Observation Radar et d'Investigation de ZONe). La portée du

radar est de 150 km dans les conditions optimales (60 km par mauvais temps : les gouttelettes d'eau en suspension dans l'atmosphère absorbent et réfléchissent une partie des ondes radars). Lors de la phase d'observation, l'hélicoptère stabilise son altitude à 4 000 m.

Des petits radars MTI transportables ont également été fabriqués. Ils pèsent moins de 100 kg et localisent au sol tout ce qui se déplace à plus de un ou deux kilomètre par heure : personnes, véhicules, hélicoptères, ULM, modèles réduits… Ces appareils sont très sensibles mais leur portée est limitée à 6 ou 8 km. Aux États-Unis, la société Lockheed a testé une version aéroportée de ce type de radar, le SLAM-R (Small Lightweight Airborne MTI Radar), monté sur un petit avion télécommandé. Le radar travaille à des fréquences comprises entre 16 et 16,5 GHz. Il ne pèse que 36,3 kg, et détecte un véhicule terrestre en mouvement jusqu'à une distance de 15 km. Ce type de radar constitue le principal obstacle à l'utilisation de véhicules terrestres. Pour la protection des sites, ces radars sont souvent montés sur des véhicules tout-terrains, couplés avec des caméras vidéo et infrarouges. Afin de détecter leur présence, il faut être muni d'un petit détecteur qui couvre les bandes de fréquence I et J de l'OTAN, c'est-à-dire entre 8 et 20 GHz. La faille de ces radars réside dans leur faible portée : il est possible de détecter leur présence avant

d'apparaître sur leur écran, donc de les contourner.

Les satellites infrarouges

Les satellites infrarouges sont les seuls appareils capables de localiser les missiles balistiques nucléaires en vol. Ces satellites munis de capteurs infrarouges travaillent dans la bande spectrale de trois à cinq µm et détectent les lancements de missiles (ou plus exactement la flamme des moteurs-fusées, qui culmine à plus de 1 000 °C). Ce sont d'ailleurs des satellites américains de ce type (série DSP : Defense Support Program) qui ont détecté les missiles Scud en vol pendant la guerre du Golfe. Ces satellites de 2,4 tonnes, placés sur orbite géostationnaire à 36 000 km de la Terre, travaillent en binôme pour localiser les tirs de missiles ou les explosions nucléaires aériennes. L'intérêt de ces gros satellites par rapport aux stations basées au sol ou aux avions est de couvrir l'intégralité de la surface de la planète de manière quasi continue.

La reconnaissance électronique passive

La reconnaissance électronique passive localise et identifie toutes les sources émettant un signal radio, des radars au talkie-walkie en passant par le GSM, la télévision et les télécommandes de jouets. Elle est

d'une importance stratégique, puisqu'elle repère au sol les avions de brouillage et d'attaque.

La collecte et l'analyse des informations sont le rôle de la NSA (National Security Agency), dotée du plus grand parc au monde de supercalculateurs.

Ne craignez cependant rien pour votre vie privée : il est impossible d'écouter toutes les communications de la planète. Et finalement, ce qui se dit importe peu : ce qui compte, c'est l'instrument détecté. Par exemple, dans les années 1970, en Angola, les services de renseignements américains constatèrent une augmentation des communications radios d'instruments utilisés généralement par les Cubains. Ils détectèrent ainsi une nouvelle arrivée de "conseillers" cubains en Angola.

De la même manière, si la France livrait des avions de chasse à un pays tiers, les émissions propres au radar de bord trahiraient immédiatement leur présence.

Ce secteur d'activité dénommé "electronic intelligence" est bien plus important que la reconnaissance optique par satellite, et bien plus secret. Mais le coût des satellites est moindre, car ils sont dix fois plus légers. Cela s'explique par les progrès incessants de la miniaturisation des composants électroniques. Les systèmes de reconnaissance électronique passive peuvent être montés sur de nombreux appareils : hélicoptères,

avions de transport, avions de combat, drones…

Les appareils de logistique

Les moyens logistiques aériens sont-ils des cibles stratégiques ?

La logistique reste la clé des conflits armés. Elle fut par exemple la cause de la défaite de Rommel en Afrique du Nord, et de l'Allemagne nazie en général.

Durant la guerre du Yom Kippour, selon le général Shazli, les Soviétiques ont livré 15 000 tonnes de matériel à l'Égypte et à la Syrie grâce à un pont aérien de 3 000 km. Ils ont effectué plus de 900 vols d'avions-cargos AN-12 et AN-22. Pendant ce temps, 566 vols de C-5 et de C-141 américains sur 10 000 km livraient 22 000 tonnes de matériel à Israël. Rapporté à la distance et au nombre de vols, l'effort logistique américain fut dix fois supérieur.

Plus récemment, la victoire écrasante des forces alliées dans le Golfe s'explique aussi par ses capacités logistiques : 500 000 hommes ont été transportés à 12 000 km de leur base, soit un mouvement de troupe équivalent à celui de la guerre du Vietnam. À une exception près, le déploiement des 200 000 premiers soldats s'est effectué en un mois et demi dans le Golfe, alors qu'il fallut neuf

mois au Vietnam !

À titre de comparaison, l'opération Overlord de débarquement sur les plages de Normandie en 1944 entraîna le déploiement d'un million d'hommes sur une distance de 200 km, soit une capacité logistique (exprimée en nombre d'hommes par kilomètre) trente fois inférieure à celle de la guerre du Golfe (source : le cabinet Mc Kinsey). Les appareils de logistique sont donc essentiels pour intervenir rapidement dans une région reculée.

Ces avions constituent une cible intéressante car ils sont chers (plusieurs dizaines, voire centaines de millions de dollars) et gros, donc visibles. La capacité de transport aérien américaine MAC (Military Airlift Command) est d'environ 80 millions de tonnes/kilomètre par jour. Soit une capacité de transport de 8 000 t/j pour une distance franchissable de 10 000 km. Ils ont 127 appareils C-5 Galaxy, 260 C-141, plus de 700 ravitailleurs en vol, et 600 transporteurs tactiques C-130 Hercules. Pour comparaison, la capacité française est constituée de 80 C-130 et C-160 ainsi que 4 DC-8.

Evaluation technologique des avions de chasse et d'attaque

Quels sont les avions militaires les plus efficaces ?

Lesquels faut-il détruire prioritairement ?

Les avions d'attaque

"Le prix des avions (durant la guerre du Golfe) n'était pas corrélé avec leur performance que ce soit en terme d'efficacité, de capacité, de fréquence des sorties, de charge emportée ou de survie."

C'est la conclusion du rapport du GAO qui s'avère sans équivoque : pour la première fois, un rapport officiel de l'administration américaine, basé sur l'analyse des documents classifiés sur la guerre du Golfe, établit qu'il n'existe pas de lien entre le prix d'un appareil et ses performances. L'analyse porte sur des faits objectifs et quantifiables, comme le coût de chaque sortie, le nombre de sorties par jour, le taux de perte par sortie et par attaque, le nombre de munitions (guidées et non-guidées) larguées, le nombre de succès par type de munition ainsi que les différentes conditions de vol et météorologiques. Le rapport montre ainsi que les résultats lors des attaques au sol sont identiques quel que soit l'âge de l'avion (années 50 aux années 80), le poids en vol (du monomoteur F-16 au B-52 de 250 tonnes), l'utilisation ou non de technologie d'invisibilité radar, de décollage vertical ou horizontal, de vitesse maximale ou de croisière…

Seule compte l'avionique, c'est-à-dire l'électronique et les détecteurs embarqués (instruments de communication numériques,

appareils de navigation GPS, pod de désignation de cible à caméra thermique…) et les armes (bombes et missiles à guidage terminal largués à distance de sécurité).

Bref, pour les attaques au sol, l'avion est simplement un transporteur de munitions. Les terroristes peuvent donc s'en prendre à tous les avions d'attaque.

Ceci dit, il y en a tellement que la destruction de tel ou tel type d'avion ne modifie que marginalement la capacité offensive d'une armée.

Le rapport de la GAO montre également que les attaques à basse altitude sont la cause majeure des pertes. En territoire hostile, l'avion volant à basse altitude doit faire face à des centaines de lanceurs de missiles antiaériens portables, à des milliers de canons et à des dizaines de milliers de mitrailleuses. Il n'existe aucune technique permettant d'éliminer ces dangers. Les appareils volant à grande vitesse et à basse altitude, pourtant caractérisés par une structure renforcée, un radar de suivi de terrain et d'évitement d'obstacle, ont les plus faibles chances de survie. Les Tornados utilisés dans ces conditions ont représenté près de 25 % des pertes totales, et ont affiché un taux de perte par sortie près de cinq fois supérieur aux autres appareils d'attaque au sol.

Si, durant l'opération Desert Storm, le commandement n'avait pas renoncé aux vols à basse

altitude, les pertes auraient été d'environ 120 appareils au lieu de 38. La différence (environ 80 appareils d'un prix moyen de trente-cinq millions de dollars) représente l'équivalent financier de 1 800 missiles de croisière (du type ALCM à 1,4 million de dollars l'unité). Bref, utiliser les avions dans des attaques à basse altitude équivaut à les considérer comme des appareils consommables.

L'arme secrète des unités de forces spéciales de l'armée américaine.

Les hélicoptères de transport des commandos.

Pour combattre un ennemi organisé, il faut être capable de déposer à bon port un nombre important de commandos. Cela nécessite un gros hélicoptère, capable de voler de longues heures, à très basse altitude, de nuit comme de jour, et par mauvais temps. Cet hélicoptère doit traverser un réseau dense de défenses antiaériennes, puis déposer une quarantaine d'hommes équipés au milieu d'une ville.

Depuis la seconde guerre mondiale, le principe des interventions rapides n'avait pas évolué : on parachutait des hommes à proximité des zones d'intervention à l'aide d'avions de transport tactique.

Le cas iranien avait montré les limites de cette technique. Le largage ne s'effectuant qu'à basse

altitude, les avions s'exposent à la défense antiaérienne. Ils constituent par leur altitude et leur faible vitesse des cibles parfaites. D'autre part, un parachutage éparpille les hommes et le matériel sur des centaines de mètres, en les laissant particulièrement vulnérables pendant une quinzaine de minutes.

En 1980, ce type d'intervention tourna au désastre. Lors du sauvetage des otages de Téhéran, les appareils des forces d'intervention de l'armée américaine se percutèrent dans le désert iranien.

L'Amérique s'interrogea alors sur sa capacité d'intervention. Reagan donna le feu vert pour une réorganisation complète des forces spéciales et du transport en territoire ennemi. Les moyens traditionnels (commandos parachutés à moyenne et haute altitude) ne suffisaient plus. Les forces spéciales de l'US Army (forces Delta…) établirent un cahier des charges de leurs besoins avec les experts de la CIA.

En décembre 1987, Boeing Helicopters livrait le MH 47E. Il s'agit d'un gros hélicoptère, le Chinook CH 47, qui a connu le baptême du feu durant la guerre du Vietnam. Il est capable de transporter 12 tonnes. Cependant, une fois équipé pour les missions d'infiltration, l'hélicoptère a une capacité de transport d'une demi-douzaine d'hommes…

Pour transporter la quarantaine d'hommes équipés

nécessaire à une intervention moderne, des hélicoptères lourds de la classe des 20 tonnes ou plus ont vu le jour. Ce sont les CH-53 Stallion, utilisés par les Marines US, le CH-47 Chinook de Boeing et le russe Mil Mi 26. Le Chinook, destiné aux forces spéciales, affiche une masse de 25 tonnes. Il est capable de voler 6 heures et peut être ravitaillé en vol. Une cinquantaine de MH-47E sont en service au sein du 160e régiment des forces spéciales de l'US Army.

Les performances techniques des gros hélicoptères.

Peu d'appareils militaires sont aptes à remplir ce cahier des charges, car les gros hélicoptères nécessitent :

- de gros réservoirs supplémentaires. Le vol à très basse altitude double la consommation de carburant ;
- un blindage contre le tir des armes individuelles ;
- un système de navigation automatique pour le vol à très basse altitude. La position est fournie par une centrale inertielle, un GPS et un système de radionavigation. Une carte précise du terrain est stockée dans l'ordinateur de bord et comparée (toutes les fractions de secondes)

à la position réelle de l'appareil ;
- un radar Doppler pour éviter les obstacles imprévus ;
- un système de brouillage électronique qui trompe les radars ennemis ;
- des leurres infrarouges qui détournent les missiles ;
- un système FLIR qui affiche en permanence une image thermique de l'extérieur (il fonctionne de nuit) ;
- des missiles air-air légers Stinger reliés au FLIR. Dès qu'un appareil apparaît, les émissions thermiques des turbines sont détectées et un missile Stinger est "calé" dessus. Le pilote peut déclencher à tout moment le tir du missile.

Les fausses cibles militaires

Les services incompétents, les matériels trop coûteux, les appareils inefficaces ne doivent en aucun cas être pris pour cibles : ce serait rendre service à l'adversaire, et le plus souvent sans même qu'il s'en rende compte. Tous ces systèmes inefficaces gaspillent une partie de la production du pays, donc détruisent une part de sa richesse. On s'étonne parfois de l'inefficacité de certaines armées, ou encore des décisions qu'elles prennent. La difficulté,

c'est que le choix d'une technologie dépend de facteurs qui souvent, très souvent, n'ont rien à voir avec l'art de la guerre.

Le général Schazli, chef d'état-major égyptien, rapporte ainsi comment on l'empêcha à la veille de la guerre du Yom Kippour d'acquérir un système d'observation particulièrement performant. Un scientifique égyptien travaillant aux États-Unis attira l'attention du général sur les possibilités des caméras IR thermiques pour repérer les conduites d'eau ou de carburant enfouies sous le sable du désert, ou encore un tank camouflé sous une bâche. L'utilisation des caméras IR thermiques aéroportées fut retardée car les services secrets égyptiens soupçonnaient l'homme de travailler pour la CIA. L'accusation était facile, mais déplacée dans la mesure où l'intérêt du système n'était en rien remis en cause. Plus généralement, les entités sociales exerçant de fortes pressions sont à l'origine de nombreux choix apparemment déraisonnables. Les pays occidentaux ne sont pas épargnés par ces dysfonctionnements.

Voici donc trois fausses cibles qui ont coûté des milliards de francs et qui pourtant n'ont aucun intérêt stratégique : le char français Leclerc, le bombardier américain B-1B et les satellites d'observation militaires.

Le char français Leclerc

En France, voici quelques années, se posa la question de la pertinence de construire une nouvelle génération de chars d'assauts : les chars Leclerc. Ces chars particulièrement performants marquent des avancées majeures par rapport aux générations précédentes. Mais leur prix de revient est bien trop élevé (supérieur à 30 millions de francs). Et le système est complètement inadapté aux conflits modernes, car il n'a aucune chance d'échapper à un groupe de fantassins armés de lance-roquettes. Ces dernières ne coûtent que quelques milliers de francs et sont utilisables jusqu'à environ 500 m. Une équation économique par trop défavorable au char, puisque le prix d'un seul modèle équivaut à celui de plusieurs milliers de lance-roquettes. Or la probabilité pour un char de survivre à dix tirs de roquettes est quasiment nulle. Les évaluations militaires les plus optimistes leur accordent une durée de vie de quelques heures sur le champ de bataille.

Pourquoi, dans ces conditions, la France a-t-elle lancé sans sourciller le programme de construction du char Leclerc ?

La réponse n'est pas d'ordre technologique ou militaire, mais plus simplement social. Les arsenaux nationaux chargés de fabriquer les armes lourdes de l'armée de terre sont éloignés des centres industriels

et commerciaux. Leur implantation a en effet été décidée dans un contexte historique où il fallait éloigner de la frontière allemande les centres de production d'armes considérés comme stratégiques.

Aujourd'hui, les chars ne sont plus des armes stratégiques, mais l'économie de régions entières dépend en partie de la charge de travail des arsenaux. Ce sont donc des groupes de pression régionaux et des syndicats qui exercent la plus lourde pression pour la continuation du programme Leclerc.

Le bombardier américain B-1B

Aux États-Unis, où le pouvoir est exercé en grande partie par le Sénat, c'est non pas la concentration des centres de production mais au contraire leur répartition dans un grand nombre d'États qui bloque les décisions.

Le programme du bombardier stratégique B-1B a été adopté malgré un coût de production très élevé, en partie à cause de la répartition de la charge de travail auprès des sous-traitants de cinquante États de l'Union.

Pourtant, il existe bien des raisons de douter des capacités du B-1B, dont le coût unitaire est de l'ordre de trois à quatre cents millions de dollars. C'est le seul appareil de l'armada américaine à n'avoir pas connu le baptême du feu lors de la guerre du Golfe.

En 1990, soit plus de six ans après sa mise en service opérationnelle, un appareil perdit un moteur en vol. Le phénomène à l'origine de cet incident fut constaté sur d'autres appareils. Tous les appareils B-1B furent donc interdits de vol du 19 décembre 1990 au 5 février 1991, soit exactement durant la période de bombardement intensive du Koweït et de l'Irak.

Selon certaines mauvaises langues, le taux de disponibilité opérationnelle du B-1B serait… nul. À tel point que la Rand Corporation propose d'économiser 20 milliards de dollars dans les 20 prochaines années en abandonnant la centaine de B-1B déjà produits et en fermant leurs bases de déploiement. En tout état de cause, le fabricant, Rockwell International (également maître d'œuvre du Space Shuttle), a pris conscience de la nécessité de répartir le travail sur tout le territoire américain afin que l'argument social fasse oublier les difficultés technologiques. Voilà comment, en rappelant que les ouvriers sont aussi des électeurs, les constructeurs emportent l'adhésion des décisionnaires sur des projets militairement contestables.

Les satellites d'observation militaires

Les satellites d'observation militaires ne sont pas utiles pour repérer les actions subversives, à cause de leurs limites physiques intrinsèques. Ce qui entrave

l'usage des satellites espions, ce sont simplement les lois de la physique : les limitations dues à l'atmosphère, à la distance et à la vitesse des satellites.

Limitations dues à la distance

La qualité d'une image est inversement proportionnelle au carré de la distance. Et les secrets militaires ont beau être bien gardés, les lois de la nature sont les mêmes pour tout le monde. Concrètement, cela signifie qu'avec la même caméra, un avion volant à 15 km d'altitude bénéficiera d'une image 400 fois meilleure qu'un satellite espion qui, lui, croise à 300 km au-dessus de nos têtes. Ceci explique naturellement pourquoi les satellites n'ont pas détrôné les avions d'observation ou les drones.

Limitations atmosphériques

Les nuages ou l'humidité dans l'atmosphère rendent inopérants les satellites munis d'un gros télescope. Il en est ainsi pour la série des satellites espions américains KH (Key Hole : trou de serrure) dont le prix avoisine la somme astronomique d'un milliard de dollars.

Ce monstre de 15 tonnes, placé sur orbite à 300 km au-dessus de nos têtes, emporterait un télescope qui

n'aurait pas grand-chose à envier au Télescope Spatial de la NASA. La définition serait de l'ordre de 10 cm. Ce monstre est en fait un dinosaure : bien adapté pour suivre les mouvements de la flotte soviétique ou l'état d'avancement de la construction d'une centrale nucléaire, il est par exemple incapable de repérer les batteries d'artillerie serbes en Bosnie.

Limitations dues à la vitesse

Plus la vitesse de l'observateur est grande, plus le temps d'observation est réduit.

Prenons le cas d'Helios. À 28 000 km/h, cet engin couvre un couloir de 15 km de côté avec une précision d'un mètre, à l'aide d'une caméra électronique et d'un télescope pointé vers la terre. À cette vitesse et avec une pareille résolution, le satellite emmagasine une quantité phénoménale d'informations. En moins de deux secondes, il explore un terrain de 15 km x 15 km. Afin de donner un ordre d'idées, pour stocker une seule image, il faudrait un CD-ROM complet, ou plusieurs centaines de disquettes.

C'est très bien d'avoir autant d'informations, encore faut-il pouvoir les transmettre au sol. Les systèmes américains ont eu recours à la technologie des plaques photographiques larguées dans l'atmosphère, ralenties par un parachute et récupérées par un avion en vol. L'autre solution consiste à

transmettre les images par ondes radios, en passant au-dessus de stations de réception. Cette contrainte impose une limitation du nombre de prises de vue (une vingtaine par jour).

Limitations dues à la masse réduite des satellites

En terme de disponibilité, le satellite est performant, car il est sur orbite et circule à une vitesse de 28 000 km/h. Encore faut-il être pourvu d'une grosse réserve de carburant, afin de changer d'orbite rapidement. C'est le cas des satellites espions américains Key Hole. Cependant, le poids de l'engin dépasse la dizaine de tonnes et le prix se compte en milliards de dollars.

Les autres, comme Hélios, balayent toute la surface du globe avec une périodicité de deux jours. En cas de problème, il faut attendre plus de 40 heures avant de disposer d'images. Durant ce laps de temps, un avion sans pilote parcourt entre 7 000 et 8 000 kilomètres. Autant dire que dans certains cas, un malheureux drone, croisant à à peine 2 km/h, arrivera au-dessus d'une région de conflit avant un satellite espion. Et il pourra demeurer au-dessus de la zone pendant deux jours sans interruption. Ce dont aucun satellite d'observation militaire n'est capable. Le coût d'un tel engin est près de mille fois inférieur à celui d'un satellite d'observation militaire.

PARTIE 5

LES ATTAQUES TERRORISTES

La plupart des objectifs militaires et civils sont fixes et répartis sur une surface d'un hectare. C'est le cas des centres énergétiques, des bâtiments, des navires situés près d'une côte, des stations radar et des sites de lancement de missiles…

Pour détruire ou endommager ces objectifs, on dispose d'un panel d'attaques que l'on trie en fonction de l'éloignement à la cible :

– les attaques rapprochées (attaques aux mortiers, embuscades, attaques aux lance-roquettes…) ;

- les attaques lointaines, à quelques dizaines, voire centaines de kilomètres de la cible (largages de bombes d'un avion, missiles de croisières, ballons utilisés pour transporter des bombes…) ;
- les attaques futuristes, telles que les attaques intercontinentales et spatiales.

D'autres attaques seront également traitées dans ces pages, comme le piratage informatique et les attaques chimiques.

CHAPITRE 1

LES ATTAQUES RAPPROCHÉES

Réussir une embuscade

Les Anglais apprirent à leurs dépens durant la Seconde guerre mondiale que les mines sont d'une redoutable efficacité pour réaliser une embuscade. Les plus performantes sont les mines antipersonnel à fragmentation. C'est l'équivalent d'un explosif entouré de milliers de billes de verre qui explose soit à l'aide d'une pression exercée sur le sol (pied ou roue), soit par une traction sur un fil. Or les légions allemandes de Rommel étaient expertes dans l'utilisation des mines en Afrique du Nord.

Voici l'histoire d'une embuscade historique qui

coûta la vie à plus d'une trentaine d'hommes.

Dans un premier temps, les Allemands placèrent des mines, sur lesquelles roulèrent des véhicules britanniques.

Les survivants sortirent des véhicules, mais l'endroit était rempli de mines antipersonnel qui achevèrent les rescapés. Une autre équipe anglaise tenta alors de récupérer les corps. Autour du lieu de l'explosion, un observateur allemand commanda un tir de mortier à distance qui surprit les Anglais. Ces derniers se réfugièrent derrière le seul obstacle naturel qui pouvait servir d'abri. Or cet endroit avait été miné et le tir de mortier était destiné à les y amener. Un nouveau carnage eut donc lieu. Avec la plus grande prudence, une nouvelle équipe britannique s'approcha des lieux du drame. Cette fois, c'est les cadavres eux-mêmes qui avaient été minés, entraînant un troisième massacre.

Attaque au mortier

Une équipe de terroristes tentant d'attaquer un site gouvernemental au mortier peut très vite se retrouver sous un déluge de feux ennemis. Aujourd'hui, on localise un mortier en quelques secondes, avant même que le premier obus ait atteint sa cible.

Pour arriver à ce résultat remarquable, les pays

occidentaux disposent de radars de localisation des pièces d'artillerie. Un des plus performants est l'AN/TPQ-36 construit par Hughes pour l'US Army. Pesant plus d'une tonne et tracté par un véhicule, ce radar est rapidement déployé autour des points sensibles. Automatisé, il scrute le ciel au-dessus de l'horizon suivant un angle prédéterminé de 90° ou 360°. Dès qu'un écho correspond à un obus de canon, le mortier est détecté. L'AN/TPQ-36 se focalise sur l'obus et détermine sa position précise à plusieurs reprises (à quelques fractions de secondes d'intervalle).

D'après les lois de la balistique, le mouvement d'un obus décrit une parabole et il suffit de connaître trois points ou plus de sa trajectoire pour déterminer précisément son équation.

Ces calculs sont effectués en temps réel par un ordinateur intégré à la station radar. Connaître l'équation de la trajectoire de l'obus permet de connaître le point de départ (où se trouve le canon) et le point d'impact.

Le radar peut localiser une trentaine de pièces d'artillerie en même temps. La portée de détection s'étend jusqu'à 15 km. Dès que les positions adverses sont connues, les pièces d'artillerie déclenchent instantanément une contre-offensive.

Une attaque au mortier n'est donc pas chose simple. Son secret réside dans le positionnement d'un

observateur avancé qui, après chaque tir, donne les indications nécessaires à l'artilleur pour ajuster le tir. On atteint ainsi une précision de quelques mètres au bout d'un minimum de coups. L'attaque peut également se faire avec un seul mortier. La précision des tirs décroît très vite si plusieurs mortiers participent en même temps à l'attaque d'un objectif. L'observateur ne peut distinguer l'origine de chaque impact d'obus.

Le radar étant incontournable, le plus réaliste consiste à se limiter à une dizaine d'obus tirés avec la plus grande précision possible, grâce à l'observateur avancé qui guidera le tir. L'opération doit être menée en moins de 15 mn. Au-delà de ce délai, le commando risque d'être repéré et éliminé. Le mortier sera placé de préférence dans une zone urbaine, pour se prémunir d'une contre-offensive et permettre au commando de disparaître dans la ville.

Une attaque au mortier nécessite aussi d'héliporter un commando à quelques dizaines de kilomètres de la cible. Il faut ensuite transporter le matériel, qui pèse parfois des centaines de kilos, près de la cible. Or, un soldat entraîné transporte au maximum 25 kg sur quelques kilomètres. Un des meilleurs moyens pour déplacer des charges lourdes sur terrain accidenté s'avère être… la brouette.

A la fin des années 60, un commando israélien attaqua une position égyptienne à Port Safaga à

l'aide de mortier de 120 mm. Le groupe avait été héliporté à une quinzaine de kilomètres de l'objectif, puis les hommes avaient parcouru une demi-douzaine de kilomètres avec le mortier et les obus, à l'aide de charrettes munies de roues de scooter, qu'ils avaient ensuite abandonnées sur place. Les autorités égyptiennes procédèrent à leur tour à des essais avec de petites charrettes à quatre roues. Ils arrivèrent à la conclusion que deux hommes pouvaient transporter ainsi 150 kg pendant quelques kilomètres en terrain accidenté.

Les précautions à prendre

Pour rechercher une personne sur le lieu d'un délit, la police scientifique s'intéresse plus particulièrement à quatre types d'indices :

– les cheveux ;
– les sécrétions (sang, salive, sperme, sécrétions vaginales et sueur) ;
– les empreintes ;
– les échantillons du sol issus de la semelle des chaussures.

Lors d'une opération subversive, le terroriste devra donc porter des chaussures neuves, des gants jetables et un bonnet.

Comment faire parler un ennemi ?

Pour faire craquer un individu, il faut le rendre fou. Comment ?

Tout d'abord, le priver de sommeil, de nourriture et de boisson. L'isoler de l'extérieur, dans le noir, pour arriver à une perte de la notion du temps. Puis réaliser des interrogatoires coercitifs sur des sujets dépourvus de sens.

L'administration de LSD après une séance de stress psychologique permet de faire parler un prisonnier.

Le LSD seul n'est pas un instrument qui détruit l'individu, mais il amplifie son état psychologique. Dans un moment de bonheur, l'effet semble positif ; dans un environnement coercitif, l'impact est très… désagréable. L'individu préfère en finir plutôt que de subir ce cauchemar.

Bref, il faut lui faire perdre la notion de temps et d'espace, faire voler en éclats les notions de norme sociale.

Méthodes de recrutement des sectes

Dans un autre domaine, les sectes, pour recruter, tentent également de couper leurs membres de la société, de sorte qu'aucun retour n'est possible.

Grosso modo, ils accueillent leurs recrues dans une ambiance sympathique pour les rassurer, créer un petit paradis. Ils prennent en charge l'ensemble de leurs besoins matériels (habillement, nutrition, hygiène, lieu de repos) pour les rendre matériellement dépendants. Ils les coupent ensuite de leur milieu social (amis et parents). Puis, les nouveaux membres sont affaiblis physiquement et psychologiquement, sous prétexte de participation à des offices religieux ou philosophiques. Ils instaurent ainsi des jeûnes, des stress permanents (bruits intermittents) et une cassure systématique des périodes de sommeil.

La soumission à des pratiques sexuelles transgresse certains tabous sociaux. Cette étape est essentielle, car les tabous sexuels sont les derniers grands tabous de nos sociétés modernes. Leur transgression isole le sujet de son corps social : s'il est tenté de retrouver son milieu d'origine, un sentiment de culpabilité (celui d'avoir transgressé des tabous fondamentaux) l'empêchera de revenir en arrière. A partir de ce moment, le sujet est un membre à part entière de la secte.

CHAPITRE 2

ATTAQUES LOINTAINES

Dès aujourd'hui, de petits groupes peuvent facilement, et pour un faible coût, construire des engins capables de voler sur des dizaines, voire des centaines de kilomètres.

Voici trois attaques lointaines que pourraient réaliser un groupe subversif :

- la construction d'un missile de 100 km de portée ;
- l'utilisation d'ULM pour bombarder des cibles stratégiques ou transporter de la drogue ;
- l'utilisation de ballons pour véhiculer des bombes sur des centaines de kilomètres.

Construire un missile de plus de 100 km de portée

Durant la seconde guerre mondiale, deux types de missiles tenaient la vedette : le V1 et le V2. D'autres programmes tout aussi intéressants ont été sacrifiés. L'un d'eux, le Blohm und Voss Bv 246, surnommé "Radieschen", était particulièrement intéressant. Ce missile pouvait parcourir près de 200 km sans moteur, simplement grâce à son profil de planeur. Lancé d'un avion à 8 000 m d'altitude, il était lâché dans la direction de sa cible. Sa finesse lui permettait d'atteindre un objectif situé à plus d'une centaine de kilomètres. Le guidage était assuré par un récepteur d'ondes radios, qui pointait le missile vers les émetteurs alliés. L'énorme avantage du planeur est sa vitesse et l'absence de moteur; il est donc peu visible au radar.

Les terroristes peuvent facilement reprendre ce type de projet, aujourd'hui élémentaire à réaliser. Les planeurs sont vendus en kit dans le commerce (50 000 à 150 000 F). Il suffit de les transformer en missiles à l'aide d'un guidage GPS (cf. "Les systèmes de guidage"), de remplir la cabine avec une centaine de kilos d'explosifs, puis de contrôler les gouvernes à l'aide d'un PC portable muni d'un récepteur GPS.

L'utilisation d'ULM pour mener des opérations subversives

Les ULM sont, au même titre que les planeurs, de bons appareils pour attaquer des cibles ennemies :

- ils sont rudimentaires, donc faciles à fabriquer. Ils sont formés d'un cadre avec un siège, des roues, un réservoir, un moteur (de 40 à 60 CV) et une hélice, montés sur un Deltaplane ;
- leur vitesse de croisière est comprise entre 80 et 110 km/h ;
- leur charge utile atteint 150 kg ;
- le pilotage est simple puisqu'on se déplace d'avant en arrière et latéralement par une barre solidaire de l'aile ;
- ils sont utilisables dans toutes les conditions atmosphériques ;
- un pilotage automatique est envisageable, en installant deux ou trois vérins électriques commandés par un ordinateur portable.

Les terroristes pourraient donc utiliser des ULM à des fins subversives :

- pour transporter de la drogue et des armes jusqu'à une distance de 1 000 km ;
- en usage offensif, pour disperser des armes chimiques ou un liquide incendiaire. La

précision requise pour ces attaques est compatible avec l'utilisation d'un système GPS pour le guidage.

On pourrait également munir les ULM de roquettes antichars (type Apilas de 4,5 kg). L'engin emporte, en plus du pilote et du carburant, une douzaine de roquettes qui atteindront leur objectif avec une précision de 5 m. Néanmoins, cette opération est risquée, car il faut obligatoirement un pilote à bord. Le tir de roquettes exige une connaissance précise de la distance séparant l'appareil de sa cible et surtout de l'orientation exacte de l'appareil. Il faut donc un pilote qui décide à quel instant précis les roquettes doivent être tirées. Or, pendant ce temps, ce pilote sera soumis aux feux des fusils d'assaut (si le site est protégé).

Contrairement aux planeurs, on ne peut pas transformer les ULM en missiles. Ils sont motorisés, donc visibles au radar, à cause de leur armature métallique et leurs hélices. De surcroît, si les planeurs suivent une trajectoire à quelques milliers de mètres d'altitude, les ULM doivent coller au plus près du terrain. A quelques centaines de mètres, les bruits du moteur, la faible vitesse de croisière et la taille de l'aile rendent les ULM facilement repérables. Les gardiens munis de fusils d'assaut ont tôt fait de les abattre avant qu'ils ne remplissent leur mission.

Construire un ballon libre capable de transporter plusieurs centaines de kilos de charge

Le ballon libre est l'un des meilleurs véhicules volants pour transporter des bombes en territoire ennemi. Il est indétectable aux radars. Il n'est pas cher à construire. Il est fiable, car il contient peu d'éléments mécaniques (moteur, système de stabilisation giroscopique), et il n'y a aucun risque d'explosion, car il n'y a pas de carburant.

L'idée est d'utiliser les vents porteurs pour emmener des centaines de kilos d'explosifs à l'aide d'un ballon au-dessus de la cible (à quelques kilomètres au-dessus). Ensuite, un système GPS accouplé à une électronique de commande (ordinateur) assure le largage de la bombe et le guidage terminal vers la cible.

Transporter des explosifs par ballon est chose simple. Grosso modo, pour un kilo de charge, il faut un ballon d'un mètre cube. Pour transporter 100 kg d'explosif, il faut donc un ballon de 100 m3.

Pour construire un ballon, une solution consiste à utiliser des sacs poubelles, c'est-à-dire des feuilles de polyéthylène de quinze ou trente microns d'épaisseurs, que l'on relie à l'aide d'une machine à soudure de plastique (à infrarouge ou aux ultrasons de préférence), matériel courant dans l'industrie du conditionnement et de l'emballage (le coût de telles

machines avoisine quelques milliers de francs). On remplit enfin le ballon d'hydrogène ou d'hélium.

Seul inconvénient : le ballon ne tient l'air que pendant la journée ; la nuit, la disparition du soleil entraîne une baisse de température et une perte d'altitude du ballon.

L'autre solution est la construction d'un ballon pressurisé rempli d'hydrogène ou d'hélium, mais fabriqué avec des couches superposées de feuilles de polyester de cinquante microns, également soudées.

Avantage : ce ballon tient l'air longtemps (jusqu'à plusieurs mois). Le cylindre représente également la forme idéale en terme de résistance au vent et à la pression atmosphérique.

CHAPITRE 3

LES ATTAQUES INTERCONTINENTALE ET SPATIALE

Aujourd'hui, les terroristes ont également la possibilité de construire, pour un prix modique, des engins capables de voler sur des distances intercontinentales, voire d'aller dans l'espace.

Appareils volant sur des distances intercontinentales

L'intérêt de construire des avions capables de voler sur des distances intercontinentales est d'utiliser des infrastructures importantes dans des lieux isolés, disposant de la bienveillance des autorités locales. Ainsi, il serait possible d'attaquer

des pays occidentaux hyper-protégés à partir du Moyen-Orient ou de l'Afrique, par exemple.

Or, la fabrication d'appareils à très longue portée par un groupe subversif est possible. En 1986, un appareil construit par un petit groupe de passionnés a effectué un tour du monde complet avec deux personnes à bord.

L'appareil, baptisé Voyager, fut entièrement fabriqué avec du papier nid-d'abeille renforcé de couches de graphite et de fibre de verre, collées à l'aide de résine. Seul le train d'atterrissage et les deux moteurs à piston (un de 130 chevaux et un second de 110 capable de fonctionner en continu pendant 10 jours) étaient métalliques. A vide, l'avion ne pesait que 843 kg, mais en charge, il dépassait les 5 tonnes, dont 85 % de carburant. Les deux pilotes, Dick Rutan et Jeana Yeager, parcoururent plus de 42 000 km en neuf jours, et bouclèrent un tour du monde complet à une vitesse moyenne de 180 km/h. Cet engin étonnant n'aura coûté que 100 000 $… et des milliers d'heures de travail bénévole.

Boeing a également réalisé un avion à hélices volant à environ 300 km/h, à 20 km d'altitude pendant 48 heures d'affilée. C'est le Condor. Son poids total est supérieur à 9 tonnes, mais la charge reste limitée à 600 kg. Pour tenir l'air à une si haute altitude, ses grandes ailes droites mesurent 61 m d'envergure.

Le DLR (organisme de recherche aéronautique allemand) a également fait construire un avion tout composite de 56,5 m d'envergure, de 13,3 tonnes, capable de voler à 18 km d'altitude pendant 48 heures. Le Strato 2C reste également quelques heures à 24 km d'altitude. La vitesse de croisière de 380 km/h est obtenue grâce à deux immenses hélices en bois à cinq pales de 6 m de diamètre.

Les terroristes peuvent donc réaliser des avions qui voyagent sur des distances intercontinentales.

Il faut pour cela :

– se procurer un avion à ailes droites, de très grande envergure, en fibre de verre et en bois (de tels avions ou leurs plans de fabrication sont vendus en kit dans le commerce) ;
– placer un réservoir de carburant représentant la majorité du poids de l'appareil ;
– intégrer un moteur à propulsion à hélices permettant une vitesse de croisière comprise entre 180 et 360 km/h.

Quelle masse une organisation clandestine peut-elle escompter mettre sur orbite?

Rêvons un peu : l'attaque spatiale

L'attaque des satellites est aujourd'hui une opération présomptueuse, mais parions que la guerre

des satellites et le terrorisme de l'espace verront le jour au XXIe siècle.

Une réussite spatiale étant le fruit d'innombrables bancs d'essais et de tirs de qualification, il ne faut guère escompter un taux de réussite supérieur à 5 %. Ce qui veut dire qu'il faut lancer au moins 20 fusées pour atteindre une cible stratégique (station spatiale ou navette) dans l'espace.

Pour construire un engin spatial, voici donc les notions initiales qu'il faut maîtriser.

En astronautique, le paramètre fondamental est la masse des objets à placer dans l'espace. La fusée la plus légère de la panoplie américaine pèse près de 20 tonnes; elle est capable de placer en orbite (basse) une charge utile de 200 kg. Grosso modo, la charge utile, donc celle des satellites, constitue 10 % de la masse totale de la fusée. Le reste est pris par la propulsion (5 %) qui permet d'ajuster l'orbite du satellite au cours de sa vie ; le carburant pour la propulsion (50 %) ; le système de stabilisation (5 %) qui évite que le satellite tourne sur lui-même ; les panneaux solaires et les batteries électriques (10 %) ; enfin la structure et divers composants tels que le système de régulation thermique.

On imagine difficilement une organisation

clandestine mettant en œuvre des fusées de plusieurs dizaines de tonnes, de plus de 20 mètres de haut, et construisant une base de lancement spatiale. Au mieux, il est raisonnable de penser qu'un engin de quelques tonnes est à la portée d'une organisation motivée. Or, l'équation qui détermine la performance d'un lanceur établit que la masse de la charge utile qui peut être placée en orbite basse dépend de trois paramètres :

- la masse de la fusée. Plus la masse est importante, plus on place de matière dans l'espace ;
- la qualité des ergols. Meilleur est le carburant, meilleure sera l'impulsion ;
- le nombre d'étages de la fusée. Plus il y a d'étages, plus la fusée est performante.

Sachant que la masse de la fusée est plafonnée à quelques tonnes, et que la qualité des ergols sera probablement médiocre, car aucune industrie spatiale ne sponsorisera l'opération ! Il n'est possible de compter que sur le nombre d'étages.

L'équation de performance impose une fusée à plus de 3 étages. En revanche, plus il y a d'étages et plus les raccords et fixations entre les étages prennent de la place. Le compromis idéal se situe, dans notre cas, à 5 étages.

En se basant sur une hypothèse de travail réaliste, on arrive à une charge utile cinq cents fois inférieure à la masse totale de la fusée.

Autrement dit, une organisation clandestine peut espérer au mieux placer en orbite basse un satellite d'une masse inférieure à 10 kg.

Caractéristiques d'un satellite offensif pour l'attaque d'une station spatiale ou d'une navette spatiale

Quel satellite d'attaque faut-il construire ?

Disposant d'une masse réduite et d'une technologie rustique, il faut renoncer à l'alimentation électrique par panneaux solaires ainsi qu'au système de stabilisation, d'orientation et de propulsion. Le satellite n'aura donc qu'une durée de vie de quelques jours, et il ne sera possible ni de l'orienter, ni de le déplacer en dehors de son orbite. Pour optimiser l'opération en fonction de ces critères draconiens, le satellite devra donc être une "mine spatiale". Il se présentera sous la forme d'une mine de quelques kilos, constituée d'explosifs, d'un dispositif de télécommande et d'une couverture de billes en céramique. Dans l'espace, quelques kilos d'explosifs entourés de milliers de billes de verre ont un effet des plus destructeurs sur un satellite ou une station

spatiale qui se trouveraient à quelques centaines de mètres ou même à quelques kilomètres. L'impact d'une seule bille peut déclencher une catastrophe.

Comme il n'est pas possible de diriger la mine spatiale, les billes de verre doivent partir dans toutes les directions et l'explosion sera déclenchée depuis le sol. Pour cela, la mine sera munie d'un bip électronique qu'une antenne parabolique au sol recevra, et qui permettra de déterminer sa trajectoire et sa position. Il faut ensuite déclencher l'explosion à l'approche d'un objet cible, comme une station ou une navette spatiale. Ces derniers objets sont visibles du sol, à l'aide d'une lunette. En général, les coordonnées de lancement des satellites sont accessibles au public. Elles permettent de déterminer la trajectoire des satellites et leur position à tout moment.

Comment construire une fusée de lancement ?

Une fusée est constituée de 3, 4 ou 5 étages. Chaque étage utilise l'un des deux types de carburant suivants : à ergols liquides ou à ergols solides. Il est illusoire de fabriquer des étages à ergols liquides. Bien que plus performante, la propulsion liquide exige des compétences techniques pointues : il faut mettre au point une chambre de combustion, une tuyère, des injecteurs, des turbopompes ou encore un

système de pressurisation. La complexité mécanique est alors telle que l'intérêt même de la propulsion liquide disparaît. En fait, la propulsion liquide est parfaitement adaptée aux fusées de plus de 80 tonnes. Pour les petites fusées d'une masse inférieure à 30 tonnes, la propulsion solide est beaucoup plus simple et donc plus efficace.

Dans ce cas, il n'y a plus aucun élément mécanique mobile. Chaque étage est un booster rempli de poudre et muni d'un système d'allumage primaire ainsi que d'une tuyère.

La poudre est difficile à mettre au point, car c'est un mélange composite : un oxydant (nitrate d'ammonium ou perchlorate d'ammonium) est associé à un combustible de la famille des plastiques aux propriétés caoutchouteuses (polybutadiènes ou polyuréthane). Ce dernier composant est d'usage courant, puisqu'on le trouve sous forme de mousse dans les sommiers et les sièges.

Ces ingrédients de base sont faciles à obtenir, contrairement aux propulseurs militaires des grandes nations occidentales. Dans ce cas, le secret de fabrication réside dans cette multitude de produits complémentaires qui font office de catalyseur à la combustion, de durcisseur ou de stabilisant. Sans ces adjuvants, le propulseur fonctionne, mais avec des caractéristiques amoindries. Pour augmenter la puissance de la combustion, on rajoute de la poudre

d'aluminium dans le mélange. Les proportions doivent être respectées avec rigueur. Par exemple, 65 % de perchlorate d'ammonium seront mixés avec 20 % de polyuréthane et 15 % de poudre d'aluminium. Dans ce cas, il faut préparer du perchlorate d'ammonium, le laisser sécher puis le broyer. Ensuite, cette poudre est malaxée avec le polyuréthane liquide et la poudre d'aluminium. La pâte ainsi obtenue est coulée dans un tube d'acier sans soudure qui servira de corps au propulseur (les soudures sont des points de fragilisation de l'acier et peuvent céder sous l'action de la combustion de l'aluminium). Il faut tasser la pâte pour éviter la présence de bulles d'air. La combustion du propulseur commencera par la base et se propagera jusqu'au bout du tube. La détermination des caractéristiques de fonctionnement des propulseurs solides est relativement aisée, puisque la poussée est proportionnelle à la surface de combustion (donc proportionnelle au diamètre du tube) et la durée de la combustion est directement reliée à la longueur du tube.

Ensuite se pose le problème de la séparation des propulseurs à poudre. Notre fusée comprend 5 étages, ce qui suppose 5 séparations successives.

Deux méthodes sont utilisées pour la séparation des étages : par des boulons explosifs ou par des ressorts. Dans le premier cas, de petites charges

explosives sectionnent les liaisons mécaniques. Cette méthode est adéquate pour de gros lanceurs, mais sur une petite fusée, la réalisation de micro-explosions est délicate et risque de déstabiliser l'engin. La seconde méthode est beaucoup plus rustique. On place de gros ressorts sous tension, bloqués par une goupille, entre deux étages du lanceur. La difficulté réside dans le fait de retirer, par un dispositif mécanique, toutes les goupilles en même temps.

Une fois la fusée lancée, le plus gros du travail reste de repérer les positions exactes de la charge et de la cible. Il faut faire appel aux technologies des liaisons hyperfréquences sur de longues distances. Ces dernières ont connu un spectaculaire développement ces dix dernières années, notamment sous la demande du marché des récepteurs de télévision par satellite.

CHAPITRE 4

LE PIRATAGE INFORMATIQUE

Les entreprises et les États se protègent de plus en plus contre le piratage informatique. Ils se défendent contre l'effraction de leurs systèmes pour assurer la confidentialité et l'intégrité de leurs données.

Un exemple classique de piratage est le sabotage des données. Les logiciels sont en effet sensibles à leur environnement. Il est donc facile de détériorer un logiciel ou un ordinateur en changeant, par exemple, les paramètres de son système d'exploitation. Un programme de quelques lignes permet le plus simplement du monde de mélanger l'action des touches du clavier. Par exemple, la lettre A devient un H.

À un niveau plus élevé, le cœur des entreprises

modernes, des administrations, est constitué par des bases de données. Ce sont les fichiers de mise à jour quotidiennes des fournisseurs et clients, des commandes, comptabilité ou encore des salaires. Si ces fichiers étaient endommagés, il en résulterait une paralysie totale de la société.

Les parades sont néanmoins faciles à mettre en œuvre. Pour minimiser les dégâts, la plupart des entreprises effectuent régulièrement des sauvegardes de tous leurs fichiers sur des bandes magnétiques, stockées dans des armoires de sécurité ignifugées. Du coup, seules les informations les plus récentes sont concernées par le sabotage.

Les actions subversives, qu'elles se fassent par l'introduction d'un virus ou par l'effacement de fichiers, ne doivent pas aujourd'hui engendrer de difficultés majeures. Seules les négligences dans l'élaboration des systèmes de sécurité informatique explique les graves dommages infligés par le sabotage informatique.

Aujourd'hui, on a beaucoup plus à craindre de l'espionnage informatique.

Pour assurer la confidentialité de leurs données, les sociétés, administrations et autres banques doivent se protéger contre les espions, concurrents, "hackers" (ces technophiles isolés)… qui pénètrent

par effraction dans les systèmes informatiques.

Comment procède un pirate pour attaquer un réseau informatique ? Il y a en fait deux types de techniques :

– celle utilisée par les “hackers”, qui agissent souvent seuls et franchissent différentes étapes pour entrer dans les systèmes informatiques ;
– la technique du “Cheval de Troie”, dont le but est d’introduire un espion dans le réseau.

La technique des “hackers”

L’effraction des hackers est virtuelle, puisqu’ils sont à l’extérieur du système informatique. C’est le réseau téléphonique qui assure le lien avec la cible.

La première étape consiste à trouver une porte d’entrée cachée. Prenons le cas d’une entreprise multinationale. Imaginons que chaque jour, un commercial à l’autre bout du monde transmet des opérations (ses ventes, ses commandes) à son siège central. Pour ce faire, il est en possession d’un ordinateur portable muni d’un modem, d’un numéro de téléphone et d’un numéro de code. Il appelle le numéro indiqué auprès de son siège. Une fois son mot de passe introduit, il accède en général à une base de données (par exemple une base de données des clients) qu’il peut interroger ou enrichir. Si le hacker connaît le bon numéro de téléphone et le bon

mot de passe, il pourra accéder à la base de données de la société multinationale.

Ses actions seront néanmoins limitées à ce que l'architecte du système informatique aura mis à disposition des utilisateurs.

Si le système informatique est bien conçu (c'est-à-dire suivant les normes actuelles recommandées en Occident), le pirate est fortement gêné dans ses actions.

Il existe néanmoins un autre type de porte d'entrée, destiné non pas aux utilisateurs mais aux gestionnaires informatiques. C'est un simple numéro de téléphone qui permet de "bidouiller" dans le système informatique. Voilà le type d'accès que recherche le pirate.

Pour le trouver, il existe différentes techniques :

– la plus simple, et certainement la plus efficace, consiste à téléphoner à un employé de l'entreprise puis à tenter de se faire passer pour un membre du service informatique. Avec un peu de chance l'employé, ne doutant pas de votre bonne fois, vous transmettra le bon numéro de téléphone et peut-être même les codes d'accès. Tout dépend de la maîtrise du "humanware" (par analogie aux software et hardware)… également dénommé la "tchatche" ;

– une autre technique consiste à tester les numéros de téléphone d'une société en éliminant les numéros classiques et les fax.

La tâche est moins insurmontable qu'il n'y paraît, car la plupart des entreprises sont équipées d'autocommutateurs privés. Ce sont de petites centrales téléphoniques intégrées à l'entreprise qui gèrent jusqu'à 10 000 lignes et autant de numéros de téléphones. Concrètement, cela se traduit par des numéros de téléphone qui commencent toujours par les mêmes chiffres, se différenciant uniquement par les quatre derniers.

Pour un ordinateur personnel muni d'un modem, rien n'est plus facile que de composer en quelques heures près de 10 000 numéros, en ne retenant que ceux qui débouchent sur le réseau informatique de l'entreprise. Ceux-ci se distinguent par l'émission d'un signal informatique sonore, un peu comme les fax. Une fois les numéros pertinents détectés, il faut les exploiter, donc passer l'écueil des mots de passe.

Fort heureusement pour les pirates, l'imagination des utilisateurs est limitée, et ce sont toujours les mêmes mots qui sont retenus. On estime que 90 % des mots de passe sont puisés dans un dictionnaire de 2 000 à 3 000 mots, commun aux utilisateurs d'un pays donné. L'ordinateur du pirate est donc programmé pour essayer tous les mots de passe du

dictionnaire que s'est constitué le pirate.

En général, l'utilisateur a droit à trois essais avant que la ligne soit coupée. L'ordinateur doit donc refaire le numéro des centaines de fois. Comme ces opérations ne réclament aucune intervention humaine, elles sont aisées à mettre en œuvre dans la pratique.

Autre technique pour trouver le mot de passe : se faire passer pour un visiteur, un stagiaire ou un membre du personnel de nettoyage, et fouiller le bureau. Soit le code d'accès est simple (par exemple, un mot, un nom ou une suite de quatre à six chiffres), soit sa complexité oblige l'usager à le noter quelque part sur son bureau. Une des raisons pour lesquelles les systèmes informatiques sont vulnérables tient à la difficulté pour les usagers de mettre en œuvre des mots de passe complexes.

Reprenons l'exemple de notre multinationale. Chaque jour, lorsque le commercial se met en relation avec le système informatique de son entreprise, il compose un code. Si ce code contient moins de six caractères (lettres ou chiffres), il est facile pour un pirate de tenter toutes les combinaisons possibles en programmant son ordinateur. Si le code contient plus de six caractères, l'utilisateur aura beaucoup de mal à s'en souvenir de tête et sera tenté de l'écrire sur papier près de son ordinateur.

Le directeur informatique de notre société se dit

donc qu'un code de six caractères est un bon compromis. En outre, le mot de passe peut comprendre des lettres et des chiffres, composant ainsi des milliards de combinaisons possibles. Notre directeur informatique aura donc la satisfaction du travail bien fait.

Or un mot de passe de six caractères est simple à "casser", car un utilisateur sur deux choisira comme code d'accès une date. Or une date est constituée de trois nombres de deux chiffres :

– le jour, c'est un nombre compris entre 1 et 31;

– le mois, un nombre entre 1 et 12;

– l'année, un nombre entre 0 et 99.

L'ensemble des possibilités (de ces trois nombres) est 31 x 12 x 100, soit 37 200 combinaisons.

A raison de trois essais par appel, il faut effectuer 12 400 appels (probablement beaucoup moins dans les faits) pour trouver un des mots clés. Avec dix appels par minute, il faut en moyenne quelques heures à l'ordinateur pour obtenir un mot de passe.

Sur le réseau mondial Internet, les hackers échangent des astuces, des dictionnaires personnels de mots de passe dont ils ont testé l'efficacité ou même des numéros de téléphone accompagnés des

mots de passe de leur victime.

Une fois la porte virtuelle ouverte, il faut encore savoir se débrouiller et circuler dans le système informatique. Heureusement, presque tous les ordinateurs qui supervisent et gèrent les réseaux informatiques parlent le même langage : les commandes UNIX.

UNIX est un système d'exploitation destiné aux stations de travail, c'est-à-dire aux ordinateurs qui se trouvent au-dessus des micro-ordinateurs en terme de puissance de calcul. Son langage de commande est enseigné dans toutes les écoles d'ingénieurs informatiques du monde. Le DOS des PC peut être considéré comme une version très simplifiée d'UNIX.

Grâce à ses connaissances des commandes UNIX, le pirate "farfouille" à son aise dans le système informatique, change les codes d'accès, liste les applications et les fichiers contenus dans le système, ouvre les applications, les fichiers, et parfois les détruit…

La technique du "cheval de Troie"

L'une des aventures les plus étonnantes de piratage informatique se déroula dans les locaux de la société informatique Digital, qui bénéficie pourtant d'une excellente réputation pour sa maîtrise

technologique des problèmes de réseaux informatiques.

Durant une période de quelques mois s'étalant sur 1988 et 1989, une pénétration "hostile" d'un réseau informatique interne fut relevée par le "SysOp", c'est-à-dire le responsable de la gestion du réseau. Par "action hostile", il faut entendre un ensemble d'interventions extérieures non autorisées qui mènent à des modifications ou à des destructions de fichiers.

Une grande enquête fut mise en branle pour déterminer la provenance de ces actions. À la grande surprise des experts, le réseau était parfaitement sécurisé et ne contenait aucune porte d'entrée accessible par des pirates. Il fallut donc reporter les soupçons sur les employés, ce qui était du plus mauvais effet sur l'ambiance de travail. Seconde surprise, il semblait bien qu'aucun employé n'ait eu intérêt à entreprendre pareille opération. Les responsables de la sécurité informatique restèrent perplexes alors que les intrusions hostiles continuaient.

Cependant, ils finirent par noter un détail troublant : le pirate apparaissait à chaque fois sur des machines bien précises, avant de se "balader" dans le réseau. Ces ordinateurs appartenaient à des employés situés dans des services différents n'ayant a priori aucun rapport les uns avec les autres. A un moment,

certains informaticiens crurent même avoir affaire à une espèce de petit génie de l'informatique qui aurait mis au point une toute nouvelle méthode de piratage faisant fi des protections les plus élaborées.

En fait, certains informaticiens avaient, de manière personnelle et non concertée, placé un modem dans leur ordinateur. Un pirate externe qui avait essayé systématiquement tous les numéros de téléphone avait découvert l'existence de ces modems "illégaux". Simple mais efficace !

La technique du "cheval de Troie" consiste donc, non plus à compter sur la négligence des employés, mais à envoyer gracieusement des modems à un certain nombre d'informaticiens en prétextant qu'ils viennent de gagner un lot après tirage au sort.

Ce type d'opération est courant. Si les experts informatiques répondent rarement à des jeux-concours, en revanche, ils visitent souvent des salons professionnels où leur nom est placé dans un fichier commercial. Rien d'étonnant donc pour eux dans le fait de recevoir un modem dernier cri. Et un sur deux se dépêchera de l'installer dans son ordinateur.

Comment une société (subversive ou non) peut-elle rendre tout piratage ou espionnage, informatique impossible ?

La première étape consiste à ce qu'aucune porte

d’accès externe ne permette d’approcher le mode de supervision (commandes UNIX) du système. Cela équivaut à n’autoriser l’accès qu’aux bases de données, à la manière du Minitel.

Pour introduire des commandes dans le système d’exploitation, il faut être présent physiquement sur place et dans un local placé sous surveillance permanente. Les portes d’accès doivent ensuite être munies d’une sécurité de rappel, c’est-à-dire que l’utilisateur appelle un numéro, donne son mot de passe, puis la ligne est coupée. C’est l’ordinateur central du système informatique qui le rappelle, à un numéro de téléphone enregistré dans une base de données référençant tout les utilisateurs potentiels.

Les mots de passe doivent enfin être fabriqués à l’aide de méthodes de construction de mots. Par exemple, le mot de passe doit être le mélange d’un nom d’animal et d’un nom de légume. Ce type de méthode met en échec les dictionnaires de mots de passe des pirates informatiques.

CHAPITRE 5

LES ATTAQUES CHIMIQUES

Les dégâts commis par les membres d'Aum le 20 mars 1995 dans le métro de Tokyo semblent considérables : 12 morts, tués par une attaque chimique au gaz sarin.

Il faut ajouter à cela une attaque manquée le 4 juillet, cette fois à l'aide de gaz cyanide (obtenu en mélangeant de l'acide sulfurique et du cyanure de sodium). Les sacs contenant les produits chimiques ont été découverts à temps dans les toilettes publics.

La secte se serait également adonnée à des essais avec des bacilles mortels d'anthrax, sans résultat, probablement à cause de la méthode d'insémination (dispersion du haut d'un immeuble dans l'atmosphère).

Potentiellement, toutes ces actions auraient pu faire des dizaines de milliers de morts. C'est du moins ce que l'on pense en ne tenant compte que de la quantité de produits toxiques.

Bien sûr, la dose mortelle de gaz sarin se compte en milligrammes. Mais dire que quelques kilogrammes de gaz peuvent tuer des milliers de personnes revient à dire que 1 000 cartouches peuvent tuer 1 000 personnes.

C'est avec ce type de raisonnement que la secte Aum a négligé l'essentiel, c'est-à-dire les moyens de dispersion efficaces, arrivant donc à un résultat assez médiocre (seulement 12 morts en négligeant les actions individuelles contre les personnes).

Entre une dispersion aérienne et une administration de substance chimique par voie orale, il existe un facteur 1 000 à 10 000.

Autrement dit, il faut près de 1 000 fois plus de produit pour obtenir, avec une dispersion aérienne, la même mortalité qu'avec un empoisonnement des aliments. De même, un produit injecté à l'aide d'une seringue sera 10 à 100 fois plus virulent et actif que le même produit avalé au cours d'un repas. Une attaque chimique ou bactériologique a donc tout intérêt à être effectuée au travers des aliments et des boissons.

L'attaque la plus efficace et la plus aisée semble être la contamination bactériologique des aliments distribués dans les chaînes de restauration rapide par

des employés complices (qui peuvent ne pas être au courant eux-mêmes de ce que qu'ils administrent aux clients).

Pour une dispersion aérienne optimale, une arme chimique doit être diffusée dans un circuit d'aération d'un immeuble ou bien à courte distance (moins de 3 mètres), directement au visage d'une personne. Cette technique aurait été utilisée par de nombreux groupes d'actions de services secrets à partir des années cinquante. Le principe consiste à pulvériser à l'aide d'un appareil idoine une grosse bouffée d'un gaz, le plus communément d'acide cyanhydrique, au niveau du visage de la victime.

Autre utilisation de la bombe nucléaire

Si une bombe nucléaire reste extrêmement difficile à réaliser, on peut l'utiliser pour ses propriétés chimiques. Avec quelques grammes de plutonium, il est possible de fabriquer une bombe chimique particulièrement dangereuse.

Une application simple serait de concentrer dans un espace réduit quelques dizaines de grammes de plutonium, qui déclencheraient un début de réaction en chaîne et surtout une émission intense de radioactivité. Avec une petite quantité de plutonium, il est possible d'obtenir une source intense de radioactivité qui peut être déclenchée à volonté. Une espèce d'explosif sans

explosion, en quelque sorte. Pour cela, il suffit de placer la quantité de plutonium disponible tout le long d'un tuyau sous formes de pastilles. Puis, on concentre la matière par un moyen mécanique à une extrémité. Commence alors un dégagement de radiations.

Le rayon d'action mortel pour ce type d'irradiation est très faible, de l'ordre de quelques mètres. Mais si on le place sous un siège, à l'entrée d'un bureau ou dans une voiture, les personnes exposées sont assurées de mourir dans les jours qui suivent sans avoir pris conscience sur le moment qu'elles faisaient l'objet d'une attaque létale.

Il est difficile de laisser l'engin tel quel lorsqu'il est activé, car en même temps que les radiations, le plutonium dégage de la chaleur. Il faut donc soit prévoir un dispositif de refroidissement, soit arrêter la réaction en éloignant les morceaux de plutonium pour laisser la matière se refroidir.

Dans la pratique, ces quelques indications d'ordre nucléaire ne suffisent pas pour concevoir une telle bombe irradiante au plutonium.

Les esprits rigoureux devront modéliser à l'aide d'un petit ordinateur le comportement du plutonium par rapport à son environnement, en faisant appel à des calculs de sections efficaces qui seuls détermineront la quantité de radiation émise en fonction de la configuration du plutonium.

PARTIE 6

ANNEXES

SATELLITES MILITAIRES

Quelle est la qualité optique des caméras d'observation placées dans les satellites par rapport aux optiques commerciales ?

Exemple 1 :

Caméra d'observation américaine

Litton ITEK PC-183

590 kg (objectif, caméra, éléments de structure et chargeur de film ou électronique CCD et système de transmission)

Focale : 1 830 mm

Ouverture : f3,7

Exemple 2 :

Caméra d'observation soviétique montée dans les

satellites espions

Caméra SA-20M (usine Krasnogorsk)

Focale : 1 000 mm

Résolution au sol : 5 mètres

Exemple 3 :

À titre de comparaison, le zoom de focale 1 200-1 700 mm de Nikon

16 kg (objectif seul)

Ouverture : f8

Champ angulaire en 24x36 : 2°-1°30

Prix : 100 000 $

À 400 km, le champ est de 7 km.

En remplaçant la pellicule par une barrette de 6 000 points, on obtient une définition théorique de 10 m au sol (1 point = 5 à 10 m).

Conclusion : ce n'est pas tant le grossissement qui importe pour une caméra montée sur satellite que les qualités optiques, c'est-à-dire la luminosité de l'objectif (qui se traduit par une valeur d'ouverture inférieure à 4).

BIBLIOGRAPHIE SUR LES EXPLOSIFS

Voici une bibliographie de référence sur la fabrication et l'utilisation des explosifs.

Un grand classique : The Poor Man's James Bond ou l'Art de fabriquer chez soi divers explosifs, poisons et autres armes à feu improvisées, par Kurt Saxon

The New Improved Poor Man's James Bond, Vo 1.Kurt Saxon, 477 p. , 1988 Atlan

The Poor Man's James Bond, Vol 2.
Kurt Saxon, 484 p., 1987 Atlan
(également publié par Paladin Press)

Les manuels techniques :

Blaster’s Handbook

Manuel d’utilisation de la dynamite édité par Dupont, un fabricant d’explosifs (explique précisément comment calculer la charge à utiliser et comment la mettre en œuvre).

Manual Of Rock Blasting

Manuel d’utilisation de la dynamite dans les opérations de démolition

Éditions Atlas

Explosives and Demolitions, U.S. Army Staff, 188 p., 1967 Paladin Press

C’est le manuel officiel de l’armée américaine (plutôt un manuel d’utilisation des explosifs militaires qu’un guide de fabrication).

Improvised Munitions Handbook, U.S. Army Staff, Technical Manual 31-210

Plus difficile à se procurer, ce guide décrit la fabrication d’explosifs avec du matériel en vente libre aux États-Unis.

Ouvrages au contenu incertain et donc dangereux :

The Anarchist's Cookbook
Paladin Press.

The Anarchist Arsenal : Incendiary and Explosive Techniques, 112 p. , 1990 Paladin Press.

Deadly Brew : Advanced Improvised Explosives, Lecker, Seymour, 64 p., 1987 Paladin Press

Explosive Dust : Advanced Improvised Explosives, Lecker, Seymour, 60 p., 1991 Paladin Press.

Ragnar's Guide to Home and Recreational Use of High Explosives, Benson, Ragnar, 120 p. , 1988 Paladin Press.

Improvised Explosives : How to Make Your Own, Lecker, Seymour, 80 p., 1985 Paladin Press

LA BOMBE ELECTRO-MAGNETIC PULSE BOMBE EMP

Faits 1

Lors de l'inauguration d'un nouveau central téléphonique entièrement électronique en Europe, les flashs des journalistes crépitèrent tandis qu'un responsable politique coupait le ruban. À ce moment précis, l'appareil se mit à présenter des dysfonctionnements. La raison de ce mystérieux phénomène ? L'alimentation électrique des flashs générait une impulsion électromagnétique.

Les centraux téléphoniques sont maintenant constitués d'un très grand nombre de circuits intégrés, du même type que ceux que l'on trouve

dans les ordinateurs. Or, la miniaturisation des circuits les rend de plus en plus sensibles aux rayonnements électromagnétiques.

Faits 2

Les radars émettent des impulsions de quelques microsecondes pour une puissance instantanée qui peut atteindre plusieurs Mégawatts. Ils sont donc (involontairement) à l'origine de nombreuses perturbations. Rappelons que le four à micro-ondes a été inventé lorsqu'un technicien américain se rendit compte que lorsque le radar de bord d'un avion de chasse était allumé, un paquet de grains de maïs placé à plusieurs dizaines de mètres était transformé en pop-corn !

Dans le même ordre d'idée, les pilotes des avions de ravitaillement en vol de l'armée de l'air américaine ne cachent pas le stress qu'ils ressentent à l'idée de ravitailler les AWACs E-3. Leur puissant radar est comme un gigantesque four à micro-ondes. Si par inadvertance le radar était en marche lors de l'approche de l'avion ravitailleur, non seulement l'électronique de bord serait endommagée, mais en plus la cargaison de kérosène transformerait l'appareil en une boule de feu.

A priori, on peut donc penser que la technologie des radars peut servir de base pour concevoir des

armes EMP. Cette solution ne semble pourtant pas faire l'unanimité des spécialistes, qui reprochent à ce genre de source de rayonnement d'être de spectre trop étroit, à de très hautes fréquences. Les obstacles comme un immeuble ou un mur sont infranchissables pour ce type d'ondes électromagnétiques.

Données techniques

Si un circuit intégré reçoit une impulsion dont l'énergie est supérieure à environ un microjoule avec une durée de vie d'une microseconde (cela équivaut à une puissance d'environ 1 Watt), il peut être considéré comme détruit. Pour une énergie 10 à 100 fois inférieure, le circuit est seulement perturbé, et le dysfonctionnement est seulement transitoire.

Sachant que le rendement (entre la puissance électromagnétique émise et celle qui est effectivement reçue par les circuits électroniques) risque fort d'être très faible, il faut disposer d'une source de rayonnement surdimensionnée, de plusieurs centaines de milliers de Watts. Inutile d'espérer avoir recours au générateur d'ondes d'un four à micro-ondes.

À savoir

De nombreux programmes de recherches

militaires ont été menés aux États-Unis pour concevoir des armes à effet EMP. Le plus simple (et le plus impressionnant) consiste à faire exploser une bombe nucléaire à très haute altitude (près de 50 km). Lorsqu'une gerbe de rayons X et de rayons gamma rencontre les couches denses de l'atmosphère (à 20 km d'altitude), des ondes électromagnétiques sont générées, couvrant tout le spectre. Ce sont ces ondes, produits indirects de l'explosion nucléaire, qui endommagent les circuits électromagnétiques. Le moins que l'on puisse dire, c'est que cette méthode, qui repose sur une attaque nucléaire dans la haute atmosphère, n'est pas très… délicate.

Dans le même ordre d'idées, il semblerait que des évaluations aient été effectuées pour mettre au point une arme EMP utilisable en centre-ville. La version nucléaire est inutilisable, car une explosion nucléaire est une émission intense de rayons X et de neutrons, qui dans l'atmosphère sont instantanément absorbés par l'air. C'est cette interaction entre les rayons intenses de la bombe et l'atmosphère qui forme la boule de feu. La difficulté consistait donc à utiliser les rayons d'une explosion nucléaire directement, en essayant de minimiser l'interaction avec l'atmosphère. C'est dans le cadre du projet "Guerre des étoiles" qu'Edward Teller, physicien d'origine hongroise et père de la bombe H américaine, proposa dans les années 80 de transformer des bombes

nucléaires en faisceau laser intense.

Le principe consistait à simplement placer une ou plusieurs barres de graphite autour d'une bombe nucléaire. Les barres de graphite devaient transformer une partie de l'énergie de la bombe en un intense rayon X. L'idée de quelques experts de l'armée américaine était d'utiliser ces faisceaux intenses pour détruire l'électronique des missiles stratégiques à distance. Mais cette idée se révéla tout simplement fantaisiste. L'atmosphère absorbe en effet exponentiellement les rayons X : au bout de quelques kilomètres, 99 % du faisceau a été dissipé dans l'air. Il ne reste pas grand-chose. D'autre part, l'énergie de l'explosion ne se retrouve qu'à environ 10 % dans les faisceaux de rayon X. Les 9/10e restants partent dans ce qui ressemble fort à une explosion nucléaire classique. En résumé, une arme EMP nucléaire n'est pas différente, dans ses effets, d'une bombe nucléaire classique. Tout comme la bombe à neutrons : pour les mêmes raisons, le concept a été abandonné.

Plan

La solution consiste à se reporter sur des ondes EM à très basses fréquences, qui se propagent beaucoup plus librement. De plus, la composante magnétique est plus aisée à produire. D'après ces

considérations physiques, une bombe EMP prend la forme de bobines inductrices (utilisées dans les moteurs électriques ou les cuves chimiques de chauffage par induction). Dans l'axe central des bobines, une puissante onde magnétique se propage avec une fréquence qui correspond à celle de l'alimentation électrique (entre quelques Hz et quelques milliers de Hz). Ce dispositif, de quelques dizaines ou centaines de kilos, sera alimenté par un groupe électrogène de quelques dizaines de kW. Monté sur une remorque, il peut être placé à quelques dizaines de mètres d'un bâtiment officiel ou même à l'intérieur ou en dessous, grâce aux égouts. La mise en marche de la bobine engendrera une très forte perturbation non seulement dans les unités centrales des ordinateurs, mais également sur les écrans vidéos ainsi que dans l'alimentation électrique. Avec une puissance d'émission de quelques dizaines de kW, les dommages sont momentanés. Mais le générateur d'ondes magnétiques reste assez puissant pour perturber les appareillages électroniques placés derrière un épais mur de béton armé. Le dispositif peut fonctionner à la demande durant des heures, voir des jours entiers.

SATELLITES MILITAIRES

Moyens de détecter les groupes terroristes
Il existe 5 types de satellites militaires :

- les satellites de technologie civile, mais destinés aux armées. Ce sont les satellites militaires de télécommunications, de météorologie et d'océanographie ;
- les satellites d'alerte. Ceux à capteurs ultraviolets et rayons X ne détectent que les explosions nucléaires atmosphériques. Ceux à capteurs infrarouges n'observent que les lancements de missiles ;
- les satellites d'aide à la radio, de navigation et au guidage (GPS) ;
- les satellites d'observation : munis de capteurs optiques ou proches infrarouges, ils ne sont utilisables que par temps clair ;
- les satellites d'écoute (télécom et radars).

Atta Oloumi

Terrorisme du XXIe Siècle : Mode d'emploi

Combien de temps encore les terroristes recourront à des techniques d'un autre âge ? Au XXIe siècle, un Etat moderne et démocratique peut-il accepter que sa sécurité repose sur la médiocrité de ses adversaires ? Si un vent de violence souffle de nouveau sur les Etats occidentaux, il risque fort de tout emporter sur son passage. Car même les imbéciles apprennent au cours du temps…

Quand les terroristes utiliseront-ils des missiles, des bombes radioactives, des armes à fragmentation, qui sont faciles à obtenir, peu onéreux, et qui pourraient faire des milliers de morts. Ces catastrophes nous pendent au nez.

Les terroristes ont aujourd'hui les moyens de déstabiliser les Etats puissants…

Atta OLOUMI, physicien Français au BIOCOMP de Stanford.USA, spécialiste de la théorie du Chaos, et attiré par tous les systèmes chaotiques, qu'ils soient physiques, économiques ou politiques.

En analysant uniquement des sources d'informations publiques, l'auteur met en évidence une fragilité troublante de notre "puissante" tranquillité.

Association Atta Oloumi

ISBN : 00100-00-0