NOUVELLES TECHNOLOGIES DE L'INFORMATION ET CRIMINALITÉ ORGANISÉE

DANIEL MARTIN*

Selon le Fonds monétaire international, le montant du retraitement des activités illégales dans le monde (trafics de drogue, d'armes, de devises, de matières précieuses, de cigarettes, prostitution, corruption, trafic d'êtres humains, de main-d'œuvre, trafic d'organes, sans oublier le terrorisme) serait de 1 500 milliards de dollars américains, soit 5 % de la richesse de la planète, ou encore 3 fois la production annuelle de l'Espagne, plus que celle de la France qui s'élève à 1 300 milliards de dollars.

En dix ans, ce sont au bas mot 3 000 milliards de dollars qui ont été accumulés par les mafias dans le monde[1]. De 1977 à 1989, plus de 800 milliards de dollars ont disparu des comptabilités nationales. Le montant des actifs boursiers des cartels de Cali et de Medellin est évalué à 10 milliards de dollars.

Le mal est donc profond, et cette manne financière qui existe doit passer d'une manière ou d'une autre dans les circuits financiers pour s'injecter dans l'économie et donner des gains propres au-dessus de tout soupçon.

DES CONDITIONS FAVORABLES AU DÉVELOPPEMENT DU CRIME ORGANISÉ

Depuis la chute du mur de Berlin et la fin de l'empire soviétique, les conditions ont sensiblement évolué.

Internationalisation des échanges, rapprochement entre économie légale et économie criminelle : les criminels ont bien intégré la mondialisation, et savent utiliser la libéralisation des systèmes financiers tout comme le démantèlement des restrictions aux mouvements financiers. Aucune règle du libre marché ne leur échappe.

L'explosion des moyens de communication et d'information, Internet et ses cousins Intranet et Extranet, ont modifié la donne.

Aujourd'hui, les matériels à disposition (PC, périphériques, puces électroniques, mémoires) sont de plus en plus puissants et coûtent de moins en moins cher. Les logiciels sont de plus en plus performants et pointus, ils touchent tous les domaines.

* Commissaire divisionnaire honoraire de la Police nationale, conseiller spécial du directeur exécutif de l'Organisation de coopération et de développement économiques (OCDE), président fondateur de l'Institut international des hautes études de la cybercriminalité (CyberCrimInstitut).

Les conclusions et opinions exprimées dans cet article sont celles de l'auteur, à titre personnel, dans le respect de la liberté d'expression. Elles ne reflètent en aucune manière la position d'un service public, d'une administration gouvernementale ou d'une organisation internationale.

Les réseaux irriguent le monde entier. On ne parle plus d'autoroutes de l'information, si ce n'est que pour rappeler les vitesses de circulation des données, mais plutôt d'un réseau tellement développé qu'il débouche, tel un chemin vicinal de nos campagnes, jusque dans nos foyers et dans l'intimité de chacun, aussi bien qu'au milieu du désert soudanais ou sur la banquise de l'Antarctique. Il suffit d'un téléphone satellite, d'un portable, et quand la communication est établie, le monde est à vos pieds.

Aujourd'hui, on est capable de faire n'importe quoi à partir de n'importe où, et cela d'une manière instantanée, à la vitesse de la lumière, pratiquement tout en gardant l'anonymat. On a réussi, de fait, à gommer les distances et le temps.

Rapidité, distance et anonymat : ces paramètres sont bien sûr de nature à favoriser le crime organisé !

Et les criminels ont vite compris l'intérêt d'utiliser les technologies de l'information et de la communication (TIC) à leur profit, soit pour continuer à perpétrer les crimes classiques avec et grâce à ce nouvel outil, soit pour commettre de nouveaux délits liés directement aux nouvelles technologies.

L'argent du crime leur permet en outre de pouvoir se payer les meilleurs matériels, sans doute aussi les meilleurs spécialistes qui peuvent travailler pour les mafias sans même le savoir, et d'utiliser les meilleures techniques du marché.

LES TIC, UN OUTIL PRIVILÉGIÉ AU SERVICE DE LA CRIMINALITÉ ORGANISÉE

Les TIC et leur utilisation intensive à travers le monde ont engendré des vulnérabilités et des menaces nouvelles dont les gouvernements, les entreprises et les individus, peuvent être les victimes (cf. annexe 1).

Les matériels peuvent présenter des failles dans leurs composants et même dans leur conception. Ces failles peuvent être placées volontairement dans les produits. On se souviendra de l'affaire Promis[2] qui dévoilait les possibilités pour les services de renseignement d'avoir accès au contenu des divers fichiers exploités dans les ordinateurs de certaines entités à l'insu de celles-ci. Mais, ces vulnérabilités concernent aussi les logiciels qui comportent des *back doors* susceptibles d'autoriser des accès intempestifs ou encore des « mouchards » renseignant sur les habitudes de l'internaute. Les réseaux constituent aussi des points faibles. On peut les écouter. Chaque point de passage de l'information peut receler un risque qu'il faut identifier et couvrir par des contre-mesures testées et efficaces.

La vulnérabilité la plus grande réside non pas dans la technique, mais dans le facteur humain. La plupart des affaires constatées montrent clairement que les malveillances proviennent, pour près de 80 % des cas, de l'intérieur de l'entreprise, et que les personnels en interne sont fréquemment associés soit à des actes volontaires, soit à de la fourniture d'information recueillie par *social ingeniering*.

Les menaces sont bien connues : piratages multiformes, pillages de fichiers, vols d'informations, destructions de données, mais aussi attaques par saturation, installations de chevaux de Troie, virus ou vers. Les sites sont vulnérables et les exemples d'attaques pullulent dans la presse sans qu'il faille accentuer encore le sentiment d'insécurité.

Les utilisateurs de ces vulnérabilités et les auteurs de ces attaques sont soit des individus, soit des entreprises (intelligence stratégique et concurrence déloyale), soit des groupes d'individus (sectes, terroristes, mafias, associations…), soit de simples personnes, qui répondent tous aux règles bien connues du « MISE » (M comme *money*, I comme idéologie, S comme sexe et E comme ego : exploiter l'orgueil, la

jalousie et les travers humains, ça marche toujours aussi bien).

Traditionnellement, le crime organisé, c'est-à-dire la réalisation d'infractions pénales par plusieurs individus en groupe suppose l'échange d'informations à tous les niveaux. Pour la préparation, souvent l'exécution du coup et ensuite la conclusion de l'affaire.

Il peut s'agir de moyens archaïques ou rudimentaires comme l'envoi de coursiers ou encore de courriers classiques et codés, on communique aussi via des pigeons voyageurs ou même des faucons. Nous savons que Ben Laden a encore utilisé ce moyen, il y a peu de temps, pour dialoguer avec le Pakistan.

Mais, le monde moderne offre des possibilités bien plus grandes : le téléphone, portable, satellite ; dans tous les coins du monde, on peut joindre quasi instantanément n'importe quel correspondant. Et l'arrivée des cartes prépayées vous garantie l'anonymat. En Sicile, dès les premières heures de vente sur le marché des cartes en question, plus de 13 000 unités ont été vendues dans la plus grande intimité, respectant la loi du silence.

Les conversations téléphoniques peuvent aussi cacher des messages d'alerte, ou organiser des rendez-vous particuliers. On a vu la mafia sicilienne préparer des coups en se donnant rendez-vous sur la tombe d'un parent. La Guarda di Finanza avait piégé la pierre tombale avec un micro miniature, c'est comme cela qu'on s'en est rendu compte !

Un coup de téléphone peut donner aussi le signal.

Un exemple récent[3]. L'affaire démarre en Russie, à Kiev, le vendredi 22 septembre 1995 à 10 heures du matin. Sergueï, industriel ukrainien compose un numéro de téléphone à Rome. La sonnerie retentit presque aussitôt dans un luxueux restaurant proche de la Piazza Navone. Fabio, le patron, un calabrais brun et massif, décroche :

« Pronto.
- Salute, c'est moi, Sergueï. Il fait beau chez toi ?
- Plein soleil, chaud, vraiment chaud !
- Tu as de la chance, ici, il fait un temps de loup.
- Et ta fille, Sergueï ?
- Superbe, je t'envoie sa photo. Elle a l'air d'une star.
- Tu veux que je l'épouse ?
- (rires de Sergueï) Tu es trop vieux mon ami !
- OK, je me contenterai de la photo. Passe-là moi sur Internet, tu connais mon adresse ».

Cette conversation, enregistrée par la section des narcotiques du centre américain de la NSA, paraît banale. Elle ne l'est pourtant pas : Sergueï est un des chefs de la mafia ukrainienne, Fabio dirige un réseau de passeurs de la Ndrangheta, la mafia calabraise, principal débouché du trafic européen de stupéfiants en provenance des Balkans et des pays de l'Est. Les enquêteurs savent qu'il s'agit d'une livraison d'héroïne, que le jour, l'heure et le lieu de livraison sont contenus dans la photo qui sera expédiée à Fabio.

Stéganographie. Aujourd'hui, tout le monde en parle. Méthode utilisée depuis longtemps par le crime organisé. Il s'agit de dissimuler un message au milieu de données numériques : son, images, fichiers divers. C'est peut-être un message en texte dissimulé dans une photo ou encore un message au milieu d'un fichier MP3. Des logiciels fort simples d'emploi existent en *freeware* sur Internet. Et comme il n'est pas possible d'essayer d'analyser toutes les photos ou tous les fichiers qui transitent sur le Web, autant dire qu'il s'agit de trouver une épingle dans une botte de foin.

Mais, ce n'est pas tout. Le meilleur moyen de ne pas se faire prendre le contenu de son message, c'est encore de le chiffrer, grâce à des algorithmes de chiffrement incassables pendant une durée de temps suffisante.

L'ETA, groupe terroriste, ne s'en prive pas, utilisant une version de PGP sûre. Le parquet antiterroriste parisien a bien des messages saisis, mais incompréhensibles.

Les criminels organisés ont compris qu'avec Internet, on risque moins de se faire infiltrer par les forces de l'ordre, et surtout qu'on a bien moins besoin de couvertures. C'est donc tout bénéfice.

Et puis la toile mondiale est si commode, il y a tellement de services disponibles qu'on aurait tort de s'en priver.

Grâce au Net, on peut jouer sur des casinos virtuels, on utilise des banques en ligne et de la monnaie électronique[4]. Vive le monde virtuel !

Il suffit d'utiliser ce qui existe. Quelques pays différents, plusieurs frontières, des méthodes légales éprouvées, et on brouille les pistes pour rendre difficile la vie des fins limiers (cf. annexe 2).

Les criminels procèdent par étapes.

Etape 1. L'argent sale est transporté du pays d'origine, par exemple la Colombie, en liquide, dans plusieurs mallettes, jusqu'à un paradis fiscal situé dans les Caraïbes.

Etape 2. Un client A des Caraïbes et un client B situé à New York, totalement indépendants l'un de l'autre, passent simultanément des ordres d'achat et de vente via un intermédiaire, gérant de portefeuille, localisé à Gibraltar.

Etape 3. Le client A et le client B spéculent sur la hausse de l'indice du marché à terme. Le client B achète « n » contrats pour une valeur nominale de « x » euros à 105 %. Il les revend tous à 105,2 %, soit un gain de 0,2 %. Le client A achète « m » contrats à 105,2 % et les revend tous à 105 %, soit une perte de 0,2 %. Mais seulement en apparence !

Etape 4. En apparence seulement car le gérant de portefeuille, situé lui à Gibraltar, demande à la société de Bourse de Paris de passer deux ordres successifs d'aller-retour. Il achète et revend en même temps « n » contrats à 105,2 % et « m » contrats à 105 %.

Etape 5. Sur le Matif, les ordres sont passés : achat-vente à 15 heures pour les mouvements à 105 %, achat-vente à 105,2 % à 15 heures 10.

Etape 6. Il ne reste plus qu'à affecter les pertes et les gains. Le client B vient de gagner 0,2 % du montant de la transaction. Par exemple, si les contrats en cause représentaient 5 millions d'euros, les gains sont de 10 000 euros. Le client B bénéficie d'un gain totalement propre. Aucun lien n'existe entre le client A et le client B.

Etape 7. Ces opérations sont bien évidemment reproductibles sur toutes les places financières de la planète : Londres, Francfort, Tokyo, New York… Il sera très difficile aux détectives de la Place de Paris de s'apercevoir de quelque chose d'anormal ou de répréhensible. Le tour est joué.

Mais, il y a encore mieux. On peut maintenant créer sa propre banque ! Et dans un paradis fiscal s'il vous plaît. Pour quelques milliers de dollars, vous pouvez en créer une au Monténégro. De préférence, choisir un pays qui est fermé à la coopération policière internationale. Pourquoi pas le Vanuatu ? 1 million de dollars suffit pour créer son propre établissement. On facture l'opération 7 000 dollars, plus la commission d'Unitrust capital, société enregistrée à Toronto. Ces mêmes Canadiens se vantent d'avoir les meilleures relations avec les banques des pays baltes qui proposent des « comptes correspondants » qui permettent ensuite des mouvements avec des banques bien sous tout rapport.

Rappelons-nous la première banque en ligne, la fameuse European Union Bank d'Antigua, proposant des produits ronflants à nos amis des Pays-Bas. Lorsque les nouveaux propriétaires russes sont partis avec la caisse (10 millions de dollars), aucun client lésé ne s'est réellement manifesté.

Le développement de l'argent virtuel va offrir encore plus d'opportunités : *smart cards*, *E-banking*, permettent des transferts rapides, véritables défis aux autorités qui poursuivent le crime.

Avec *eGold*, installé dans l'île de Nevis aux Caraïbes, on peut acheter en ligne de l'or virtuel. Cette société annonce 200 000 clients pour une gestion de 14 millions de dollars[5]. Ce site est certainement utilisé par des blanchisseurs car l'anonymat y est garanti. Les technologies de la finance n'ont plus aucun secret pour les mafias[6].

Plus récemment, on sait que les terroristes islamiques utilisent les mêmes types de réseau pour financer leurs actes (cf. annexe 3).

Tout ceci paraît bien facile. Comment réagir ? Sommes-nous totalement démunis ?

Les TIC, au service de la riposte

Face à la rapidité des transactions et à un espace géographique planétaire, nous opposons[7] un univers découpé en territoires souverains, avec des lois et des pratiques différentes, voire contradictoires. Un policier, un juge, ça exerce avec une compétence territoriale précise. Or, on constate que toutes les transactions criminelles passent par de multiples pays aux lois différentes, quand elles existent !

Rappelez-vous « *I love you* ». Le virus fait le tour du monde en un temps record. Un succès mondial, des milliers d'ordinateurs saturés, des pertes financières non négligeables. Pax Americana oblige, le FBI américain vient en aide à son collègue philippin. Un jeune est arrêté. L'auteur de la vague infectieuse. Il est rapidement relâché… faute de texte réprimant de telles activités sur le sol des Philippines. Les Américains rentrent chez eux. Il reste à voter une loi sur place…

Mais tout de même, si on a pu réagir dans des délais assez courts, c'est que nous ne sommes pas démunis totalement.

Pour des raisons techniques, des traces existent. D'abord, pour établir les connexions via des fournisseurs d'accès et des hébergeurs, puis pour que les messages arrivent à bon port et établissent un lien entre l'envoyeur et le destinataire. Ensuite, pour que la maintenance des réseaux s'effectue en cas de panne, mais aussi que les éventuelles facturations soient possibles.

Si des traces existent, alors on peut les remonter.

Et voici posées les questions fondamentales. Qui va garder ces données numériques de transactions ? Qui va payer le prix de cette conservation ? Quel délai de conservation ? Qui va avoir accès ? Qui va contrôler ces accès pour garantir les libertés individuelles ?

D'autres questions tout aussi pertinentes. Quid des perquisitions transfrontières ? des délais d'entraide judiciaire ? Veut-on faciliter l'efficacité, sacrifier la souveraineté ? Quelle confiance ?

Pour la première fois, une réponse est en train de s'élaborer : le Conseil de l'Europe vient de mettre au point une Convention de lutte contre la cybercriminalité[8]. Un texte qui tient, enfin, compte des différences culturelles et qui n'impose pas, mais qui propose. Des grands principes qui doivent ensuite passer dans le droit interne des pays signataires, mais en respectant la culture locale. Il reste qu'il faut du temps pour ratifier et appliquer.

Plus directement opérationnels, il faut parler des travaux du G8 sur le *High Tech Crime*. On a enfin compris que la coopération, c'est 24 heures sur 24 et 7 jours sur 7, que chaque pays doit mettre à disposition des troupes formées et capables de répondre dans l'instant. Mais, le travail est encore long car il faut respecter les sensibilités de chacun.

A moins d'un électrochoc. Et nous venons d'en subir un violent.

Alors, on voit surgir des outils inavoués. *Big Brother* est de retour. Echelon, ce réseau, susceptible d'engranger et de filtrer l'équivalent du volume de la bibliothèque du Congrès toutes les trois heures, mouline à fond. Carnivore, installé en urgence sur les serveurs, surveille les E-mails ; Cyber

détective, Net détective, autorisent des fonctions incroyables et permettent de vérifier l'activité de n'importe quel internaute de la planète. Certains logiciels permettent même de capturer les données au moment où on les frappe sur le clavier, et donc avant qu'elles ne soient chiffrées ! On le voit, les outils sont nombreux qui permettent de tout surveiller, mais aussi de faire de l'espionnage économique, de malmener les règles d'une juste concurrence. Tout dépend comment on va les employer. Quelle éthique, quelle déontologie ? Jusqu'où aller ?

Question de volonté politique, sans aucun doute.

Des structures existent pour faire face à certaines activités criminelles dont le blanchiment : le Gafi[9] a élaboré des recommandations, il dresse maintenant des listes noires, il dénonce des comportements et examine des *modus operandi*. Il permet l'évaluation des procédures. Dans chaque pays, des « Tracfin »[10] se mettent en place. Est-ce suffisant ? Quels sont les résultats en matière judiciaire, quel frein au crime organisé ? Difficile à mesurer.

VERS QUEL AVENIR ?

Il reste que nous sommes dans un processus, et que ce processus est en marche. Il ne demande qu'à s'améliorer. Dans quels secteurs ?

Celui de l'accroissement de la coopération internationale. Les divers partenaires doivent apprendre à mieux se connaître, à mieux dialoguer, à mieux communiquer. Nous avons les TIC, utilisons-les. Mais, il faut que les personnels se connaissent, qu'un climat de confiance s'établisse. Il faut créer des points de rencontre. Privilégier les contacts humains et les échanges. L'Office européen de police (Europol) répond à ce besoin. Pour autant qu'il existe une structure ou une organisation criminelle, et que plusieurs Etats membres soient affectés. Une autre structure pourrait être mise en place rapidement. Un « Gafi plus ». Il s'agirait d'un super Gafi dans lequel travailleraient notamment des experts du renseignement, et qui prendrait un tour plus opérationnel. Car aujourd'hui, le Gafi a pour mission, après avoir élaboré quarante recommandations dans le domaine du blanchiment, de passer au crible les arsenaux législatifs que les pays mettent en place pour lutter contre ce phénomène et de dresser la liste des pays contrevenants, à mettre au banc des mauvais élèves. L'outil n'est pas suffisant pour venir à bout du financement des activités terroristes. Il faut le muscler.

Formation, sensibilisation des acteurs. La formation ne doit pas être l'enfant pauvre des dispositifs. N'oublions jamais qu'en face, on est capable de se payer les meilleurs spécialistes. Une vraie gestion des ressources humaines doit accompagner une vision à long terme. On voit encore trop souvent des agents obligés de quitter un poste, où ils sont bien formés, pour obtenir une promotion. Il faut alors recommencer à zéro. La sensibilisation mérite aussi sa part. Un homme prévenu en vaut deux. A tous les niveaux, il faut répéter le message.

Faire un effort au niveau des structures. Pour l'instant, chaque ministère travaille dans son coin. Une organisation transversale du travail est pourtant nécessaire. Au lieu de saupoudrer les moyens, il vaudrait mieux les regrouper, établir des équipes complémentaires et spécialisées, composées de fonctionnaires issus de tous les corps et assistés de personnels du secteur privé, mieux à même de faire face à la modernité. Il convient de doter ces structures de moyens matériels suffisants. La Grande-Bretagne vient de créer une unité de lutte contre le crime de haute technologie. Quatre-vingts personnes y sont déjà affectées, et un budget conséquent attribué.

Une véritable réforme du secret bancaire est absolument obligatoire si on veut

réellement éradiquer les problèmes de blanchiment à terme, qu'il s'agisse de terrorisme ou de criminalité classique ; il va falloir des efforts considérables pour que, sur un plan international, nous soyons d'accord sur le sens des mots. Il suffit de voir la polémique actuelle provoquée par le rapport parlementaire français sur les pratiques anglaises et la notion de paradis fiscal, pour se rendre compte que le chemin sera long.

Une nécessaire volonté politique d'aboutir sans laquelle tout ceci serait totalement inutile. C'est donc notre devoir, sans se lasser, de sensibiliser aussi le pouvoir politique, de lui ouvrir les yeux, d'obtenir des budgets et de financer des projets à long terme. On lutte contre la criminalité organisée comme à la guerre. Il faut donc des budgets pluriannuels comparables à ceux consacrés aux armées classiques. Sans argent, pas de moyens ; sans moyens, peu de résultats et aucune consolidation dans le temps.

Ainsi des réactions sont en marche. Mais, nous connaissons bien les limites des réglementations et législations nationales empêtrées dans les notions de territorialité et de souveraineté. D'un côté la modernité, de l'autre le moyen âge avec ses octrois. Nous connaissons également bien les difficultés des organisations internationales qui ont besoin de temps pour obtenir le consensus et qui accouchent souvent d'une souris. Ne parlons pas des délais de mise en place pratique des décisions. En attendant, le crime avance.

Alors, je crois que nous ne pouvons pas rester les bras croisés et que des initiatives sont indispensables. Nous ne pouvons pas nous contenter des réactions purement étatiques. C'est la raison pour laquelle il convient de signaler des initiatives privées.

D'abord, certains agents ou fonctionnaires d'Etat, tous impliqués dans la lutte contre le crime, ont eu l'idée de se regrouper en réseau, réseau international et protégé, dédié aux questions pratiques que se posent les enquêteurs : policiers, magistrats, douaniers, gendarmes, agents de la concurrence et des prix… Une question pratique sur un logiciel, un ennui technique, un éclairage, et il y a toujours quelqu'un du réseau pour apporter une ou plusieurs réponses utiles. Plusieurs pays, plusieurs sensibilités, plusieurs cultures, derrière une même éthique au service de l'efficacité. Ça marche ! C'est au moins une solution à creuser.

Autre initiative : la création du CyberCrimInstitut ou Institut international des hautes études de la cybercriminalité.

Ses missions sont ambitieuses. Il s'agit de tout mettre en œuvre pour :
- accroître la connaissance de la criminalité de haute technologie mettant en cause les nouvelles technologies de l'information, tant sur un plan national qu'international et dans toutes les dimensions qui menacent nos sociétés : juridiques, criminologiques, sociales, culturelles, économiques, financières… ;
- apporter, après avoir conceptualisé les éléments caractéristiques des menaces de toute nature, des propositions concrètes visant à créer ou renforcer les moyens de lutte contre cette forme de criminalité, tant au niveau des services gouvernementaux que du secteur privé ou des citoyens ;
- permettre, au niveau national, européen et mondial, un réel dialogue entre toutes les parties concernées (secteurs publics au sens large, entreprises privées, associations et représentants des citoyens et consommateurs) en vue d'élaborer des parades communes en favorisant les échanges, tout en garantissant la protection de la vie privée et des consommateurs ;
- développer une activité d'étude et de recherche, de documentation, d'analyse, de prospective, de communication, d'alerte et de proposition sur ce sujet, au sens le plus large et par tous les moyens disponibles existants ou à venir, afin de favoriser les échanges et voyages d'étude, et d'une manière générale l'établissement d'un véritable courant d'information ;

- proposer d'organiser et de diffuser une activité d'information, de sensibilisation et de formation sur ce sujet, en particulier par la tenue de colloques, conférences, forums ou symposiums ;
- apporter dans l'ordre national, communautaire et international, une réflexion transdisciplinaire et des propositions concrètes de riposte ;
- constituer un lieu de rencontre où acteurs et observateurs impliqués dans ce domaine peuvent développer, dans un cadre neutre, un dialogue serein ;
- nouer et entretenir tous les contacts utiles en vue de répondre à ces objectifs ;
- mettre les nouvelles technologies de l'information et de la communication au service de l'homme en prévenant la prolifération des sanctuaires informatiques, refuges des criminels, et en luttant notamment contre le blanchiment d'argent et la corruption qu'ils engendrent.

Le CyberCrimInstitut compte agir :
- par l'intermédiaire de *Task Forces* ciblées ;
- en prospectant les secteurs-clés ;
- en influant sur les acteurs essentiels : gouvernants, politiques, chefs d'entreprise, décideurs à tous les niveaux ;
- en sensibilisant et en formant les partenaires publics et privés ;
- en constituant un réseau d'experts de tous les milieux : universitaires, industriels, commerciaux, militaires, diplomates, fonctionnaires…

Face à la prolifération du crime organisé, il semble bien que de nouvelles ripostes soient nécessaires, et qu'il faille remettre en question le train-train auquel nous étions habitués jusqu'à maintenant.

Il devient impératif de constituer un front capable d'améliorer considérablement l'efficacité. Aussi, il faut gommer les sujets de discorde pour accentuer nos points communs et les mettre en valeur. Sans doute, faut-il créer une véritable base de données centralisée mondiale sur le crime organisé, bien protégée et accessible uniquement aux personnels ayant le besoin d'en connaître. Aujourd'hui, plusieurs organisations sont concurrentes et n'intègrent pas toutes les données. Les unes sont purement européennes, les autres sont seulement judiciaires et occultent une fonction pourtant fondamentale, celle du renseignement. Il faut accepter de partager l'information !

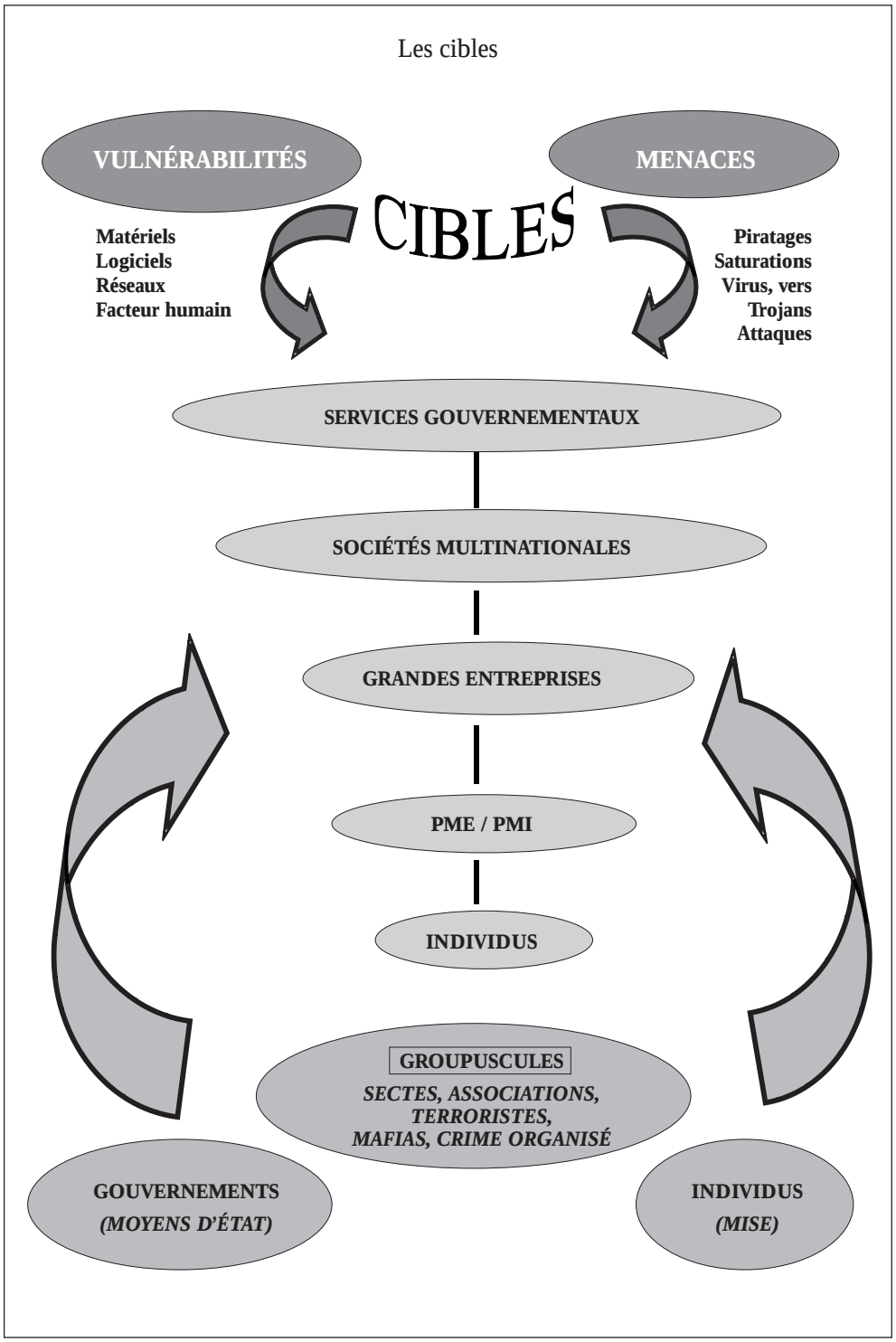
Il devient aussi indispensable de revoir les vieux concepts de sécurité intérieure opposée à la sécurité extérieure. Aujourd'hui, la sécurité est un concept global qu'il convient d'appréhender dans toutes ses dimensions. Les moyens sont limités, alors il faut redéployer et éviter les redondances et les querelles de clans.

De la même manière, il faut effectuer un recentrage des métiers. Un juge doit rendre la justice, un policier rechercher les auteurs des infractions pour les remettre à la justice, il n'est pas un correspondant social. Chacun à sa place. Aussi, on ne pourra pas continuer éternellement d'effectuer un transfert sur d'autres métiers. Un banquier, un assureur, un notaire ou un avocat, ne sont pas des « flics ». Leur demander un travail pour lequel ils ne sont pas faits, ne peut pas conduire à régler les difficultés.

Il est urgent de faire face à nos responsabilités et de faire preuve d'imagination. Sans doute, les derniers événements sont là pour nous rappeler le proverbe de Salvador Dali : « Le coup de pied au cul, c'est l'électrochoc du pauvre ».

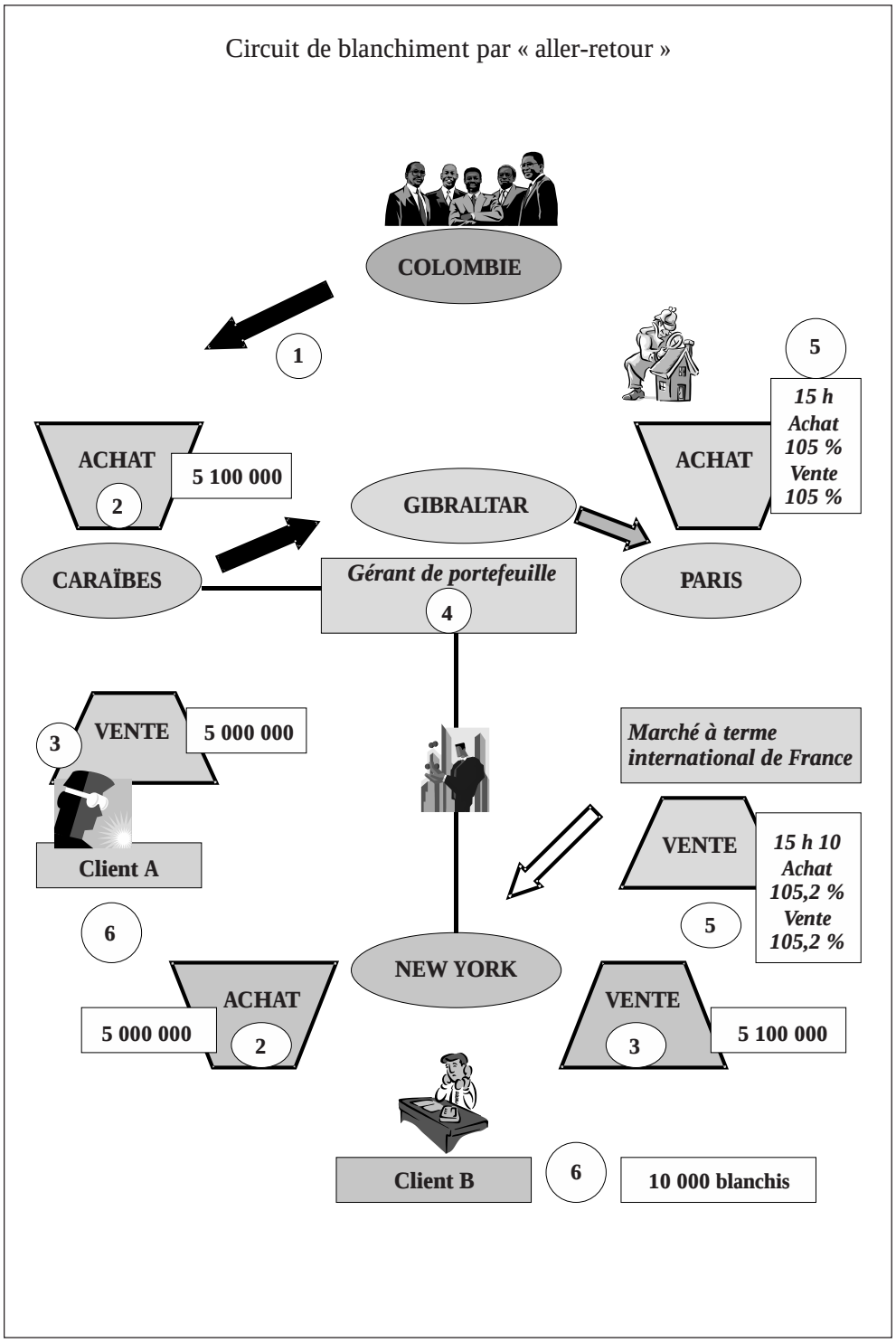
Alors réveillons-nous !

ANNEXE 1

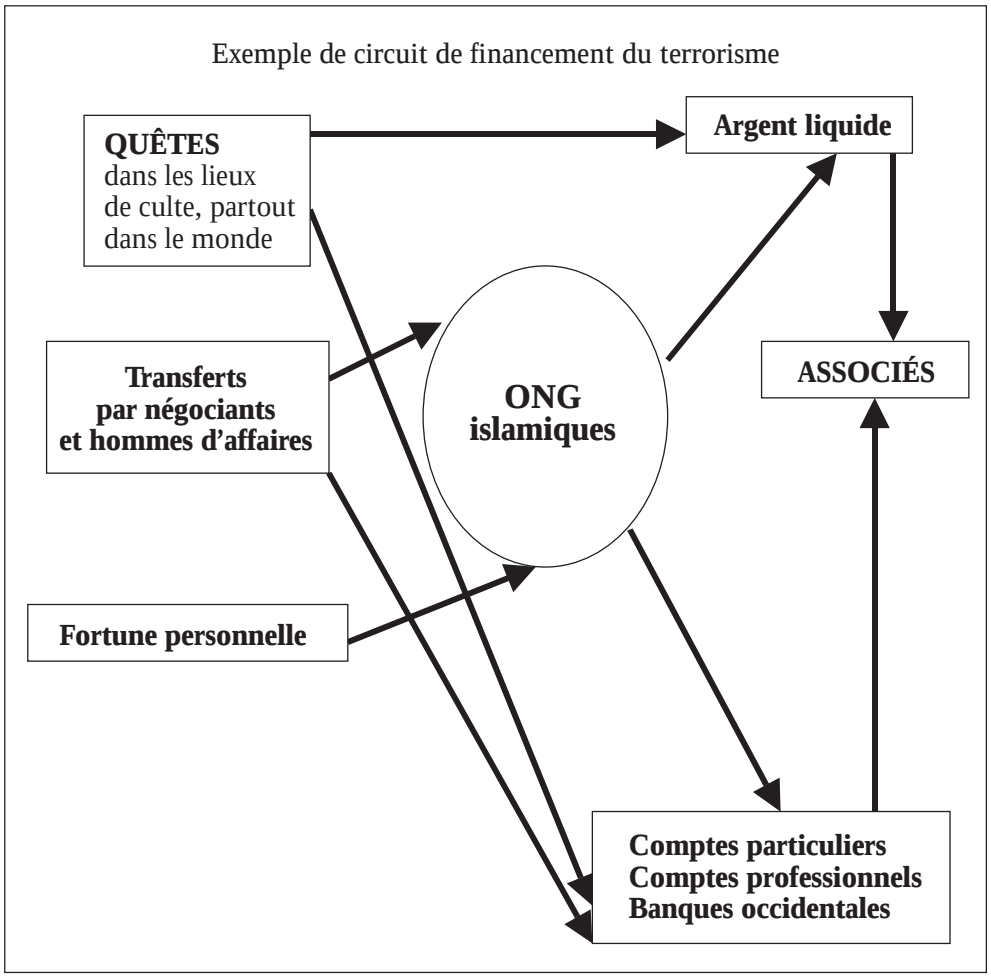

Les cibles
VULNÉRABILITÉS
MENACES
CIBLES
Matériels
Logiciels
Réseaux
Facteur humain
Piratages
Saturations
Virus, vers
Trojans
Attaques
SERVICES GOUVERNEMENTAUX
SOCIÉTÉS MULTINATIONALES
GRANDES ENTREPRISES
PME / PMI
INDIVIDUS
GROUPUSCULES
SECTES, ASSOCIATIONS,
TERRORISTES,
MAFIAS, CRIME ORGANISÉ
GOUVERNEMENTS
(MOYENS D'ÉTAT)
INDIVIDUS
(MISE)

ANNEXE 2

Circuit de blanchiment par « aller-retour »



ANNEXE 3



NOTES

1. *Un monde sans loi* (éd. Stock) de Bertossa, Gialanella, Dejemeppe, Van Ruymbeke, Joly, Vichnievsky.
2. Voir à ce sujet le livre de Fabrizio Calvi et Thierry Pfister, *L'œil de Washington*, Albin Michel, 1997.
3. Voir *Criminalité informatique*, Daniel Martin, PUF, 1997.
4. Voir, à ce propos, les rapports du Gafi disponibles en ligne sur le site www.oecd.org rubrique blanchiment de capitaux.
5. Source USA Today.
6. Voir à ce sujet la revue *Futures*, n° 9, octobre 2001.
7. Lire *Cybercrime : menaces, vulnérabilités et ripostes* de Daniel et Frédéric-Paul Martin, PUF, juin 2001.
8. Texte de la Convention disponible sur le site www.coe.int
9. Le Gafi est le groupe d'action financière contre le blanchiment d'argent dont le secrétariat est abrité par l'OCDE.
10. Tracfin est la cellule du Traitement du renseignement et action contre les circuits financiers clandestins, dépendant du ministère de l'Economie et des Finances.