Collège Interarmées de Défense

TERRORISME ET GEOPOLITIQUE

MODES DE FINANCEMENT DU TERRORISME

Mémoire de géopolitique

DE

LCL. AMER AHMED

1 4ème promotion

DE L'ARMEE DE TERRE EGYPTIENNE

Directeur de Séminaire :

M. François Géré

MARS 2007

Sommaire

MODES DE FINANCEMENT DU TERRORISME

Première partie

Un aperçu sur le terrorisme

Le terrorisme, l'origine, les causes, et les méthodes pour réaliser ses missions, et la situation générale après 11 Septembre dans le monde.

Deuxième partie

Les sources du financement d'activités terroristes

Différentes sources du financement d'activités terroristes, Les transferts de fonds et la relation entre blanchiment d'argent et financement du terrorisme

Introduction

Le mot **terrorisme** est employé pour la première fois après la Révolution Française. Il se rapportait au régime de **La Terreur** Mais les phénomènes que l'on connaît aujourd'hui sous le nom de terrorisme sont bien différents. Désormais, on appelle terrorisme une stratégie de lutte, de guerre, que choisit le plus faible pour combattre un adversaire plus fort militairement.

Les guerres sont nombreuses et les exemples de terrorisme aussi : Irlande du Nord, Corse. De quoi s'agit-il ? De groupes de personnes, politiquement organisés, qui décident de faire des **attentats**, c'est-à-dire des actions violentes contre des personnes ou des biens appartenant à leur ennemi déclaré. Le terrorisme est une stratégie pour rendre visible un état de guerre qui parfois ne l'est pas. C'est une forme de guerre en fait.

Et, parce que ce sont des cibles plus faciles à toucher, les objectifs des attentats peuvent parfois être des civils, de simples citoyens de l'Etat contre lequel les terroristes sont en guerre.

Le terrorisme est une façon de démontrer que la guerre existe ou d'attirer l'attention sur des désirs de changement. Les terroristes utilisent donc la violence la plus visible possible, pour faire peur à leur ennemi. Souvent ils espèrent que la terreur de la population contraindra leur adversaire à négocier avec eux ou à changer d'attitude. Les terroristes défendent des causes, des idéaux, parfois justes au travers d'actions terribles, injustifiables (comme toute guerre).

Le blanchiment de capitaux et le financement du terrorisme soulèvent de gros problèmes en matière de prévention, de détection et de poursuite pour une grande partie des pays.

Les techniques sophistiquées utilisées pour blanchir des capitaux ou financer le terrorisme rendent ces problèmes plus complexes encore.

Ces techniques sophistiquées peuvent impliquer différents types d'institutions financières ; de nombreuses transactions financières utilisant plusieurs institutions financières ou d'autres organismes tels que des conseillers financiers, des sociétés-écrans et des fournisseurs de services comme intermédiaires ; des transferts, via et vers différents pays ; et l'utilisation de nombreux instruments financiers et autres types d'actifs à accumulation de valeur. Le blanchiment de capitaux est toutefois un concept assez simple.

Il s'agit d'un procédé par lequel le produit d'une activité criminelle est déguisé pour cacher son origine illicite. Au fond, le blanchiment de capitaux concerne davantage le *produit* de biens d'origine criminelle que les biens eux-mêmes.

Le financement du terrorisme est également un concept simple à la base.

Il s'agit du soutien financier, quelle qu'en soit la forme, du terrorisme ou de ceux qui le soutiennent, le planifient ou le commettent.

Il est toutefois moins facile de définir le terrorisme lui-même car le terme peut avoir d'importantes implications politiques, religieuses et nationales qui diffèrent d'un pays à l'autre.

Le blanchiment de capitaux et le financement du terrorisme présentent souvent des caractéristiques transactionnelles similaires, la plupart étant liées à la dissimulation.

Les blanchisseurs de capitaux envoient des fonds illicites par des voies légales afin de cacher l'origine criminelle de ceux-ci alors que les personnes qui financent le terrorisme transfèrent des fonds qui peuvent avoir une origine légale ou illicite de manière à cacher leur origine et leur utilisation finale, qui est le soutien au terrorisme.

Le résultat est cependant le même : la récompense.

Une fois les capitaux blanchis, les criminels sont récompensés par un produit déguisé et apparemment légitime.

De même, ceux qui financent le terrorisme sont récompensés en apportant un soutien financier visant à mettre en place des stratagèmes et des attaques terroristes.

Première partie
Un aperçu sur le terrorisme

Dans cette première partie je vais exposer quelques caractéristiques sur le terrorisme et les différentes méthodes et moyens, pour imaginer les moyens financiers pour ces opérations. Notamment le 11 Septembre qui a changé beaucoup d'éléments pour faire face à ce phénomène.

1.1 TERRORISME

Il est beaucoup question de terrorisme depuis la fin des années 1960, et plus encore depuis le 11 Septembre 2001. Tout le monde en parle, tout le monde appelle à combattre ce fléau. Mais qu'est-ce au juste que le terrorisme ?

Les définitions ne manquent pas. Aux Nations-unies, malgré des années de discussion en vue d'aboutir à une convention internationale, il n'a pas été possible de se mettre d'accord sur la signification de ce terme. Dire, comme le fait le *Petit Larousse*, qu'il s'agit de *"l'ensemble des actes de violence commis par une organisation pour créer un climat d'insécurité ou renverser le gouvernement établi"*, c'est ne prendre en compte qu'une partie du problème.

Un des deux points de divergence au sein de l'ONU réside précisément dans la distinction à faire ou à ne pas faire entre organisations terroristes et mouvements de libération. L'autre a trait au terrorisme d'Etat, dont certains vont jusqu'à nier l'existence.

1 .2 LES ORIGINES

La première utilisation du mot "terrorisme" - dans un sens assez différent de celui d'aujourd'hui remonte à la révolution française, à Robespierre et à son régime de justice expéditive. C'est ce que le chef des Jacobins appelait lui-même *"la terreur sans laquelle la vertu est impuissante"*,

S'agissait-il de terrorisme d'Etat ou de violence exercée par un groupe politique sur un autre afin d'imposer un changement radical ? On en a longuement débattu, on pourrait en débattre encore. Le phénomène s'est reproduit plus d'un siècle plus tard avec la révolution russe de 1917, en s'amplifiant considérablement. **La "terreur rouge", élevée au rang de vertu révolutionnaire en réponse à la "terreur blanche", a longtemps survécu à cette dernière.**

Mais la terreur institutionnalisée de Robespierre ou de Staline - on en parle d'autant plus qu'eux-

mêmes se sont vantés de la pratiquer - n'a pas été la première qu'ait connue l'histoire humaine. La crucifixion de milliers d'esclaves dans la Rome antique ou l'extermination de centaines de milliers d'Indiens d'Amérique sont antérieures. Il est vrai toutefois que ces excès passent rarement pour des actes de terrorisme. Pas plus que le massacre de 30.000 Parisiens, perpétré par les tueurs versaillais d'Adolphe Thiers en mai 1871, sous l'œil bienveillant de l'occupant prussien.
En revanche, les assassinats individuels de rois, de princes, de présidents, d'hommes politiques, d'industriels ou de banquiers, tels qu'ils se pratiquent depuis le 9ème siècle, sont considérés comme terroristes.

1 .3 Causes et motivations de terrorisme

1- extrémisme religieux et idéologique
2- extrémisme nationaliste
3- extrémisme politique
4- extrémisme criminelles

1.4 Méthodes du terrorisme

On retrouve une constante dans le terrorisme: les méthodes utilisées. La plupart des organisations terroristes ne sont pas au point de vue tactique innovatrices et dévient rarement de leur *modus operandi*. Elles s'en tiennent essentiellement aux méthodes principales du terrorisme: l'attentat à la bombe, l'assassinat, la prise d'otage (incluant l'enlèvement) et les atteintes à la sécurité des transports.

Ces méthodes peuvent être cataloguées en deux catégories: les *events of duration* et les *conclusive events*. Dans la première catégorie, on retrouve la prise d'otage et les détournements d'aéronefs. Ces méthodes sont souvent d'une longue durée et impliquent une négociation, ou du moins une discussion, entre les auteurs de l'acte terroriste et les autorités. Dans la seconde catégorie, on retrouve comme méthodes celles qui visent à tuer ou blesser, et qui surviennent trop rapidement pour permettre une réaction de la part des forces de l'ordre: l'attentat à la bombe et les assassinats

Elles se réduisent à trois types:

a) les méthodes qui visent les biens (attentats à la bombe contre des bâtiments et des véhicules).

b) les méthodes qui sont dirigées contre des personnes et leur liberté (les prises d'otage) ou leur intégrité physique (assassinats sous diverses formes).

c) les méthodes qui frappent à la fois les personnes et les biens matériels (les détournements d'aéronefs).

1.4.1 **Attentats à la bombe**

Les attentats à la bombe constituent un problème important pour la sécurité publique. Chaque année, des centaines de personnes sont tuées ou blessées par ces attentats. Ils sont aussi responsables de dommages matériels se comptant en millions de dollars.

Les attentats à la bombe sont l'œuvre de diverses sources: individus déséquilibrés mentalement, individus auto-motivés, groupes criminels organisés et terroristes. Les attentats commis par des individus déséquilibrés sont sans motif apparent et ils sont perpétrés pour le sentiment de puissance et d'excitation qu'ils procurent. Quant aux groupes criminels organisés, ils utilisent les attentats pour intimider et assassiner certaines personnes pour acquérir des gains financiers et contrôler certaines activités criminelles. Les attentats à la bombe perpétrés par les bandes de motards criminalisés contre leurs concurrents constituent de bons exemples. Les terroristes, pour leur part, ont recours aux attentats à la bombe à des fins politiques et idéologiques.

Dans les dernières décennies, les terroristes ont utilisé essentiellement l'attentat à la bombe comme méthode criminelle contre une variété de cibles: ambassades, missions commerciales, grandes entreprises, administrations gouvernementales, forces de l'ordre, centres touristiques, marchés publics, etc. On estime que les attentats à la bombe constituent près de 80 % des actes de terrorisme.

1.4.1.1 **Types d'attentats**

Les attentats à la bombe peuvent être divisés en deux catégories: les attentats symboliques et les attentats anti-personnel :

Les attentats symboliques ont comme objectif premier de rendre médiatique une cause. Ils sont perpétrés contre des cibles qui ont une connotation symbolique. Ceux qui les commettent préfèrent éviter d'infliger des blessures physiques pour ne pas s'aliéner le support du public. Ils peuvent être perpétrés durant la nuit. Ils sont de façon générale précédés d'un appel de mise en garde afin de

permettre aux personnes concernées d'évacuer les lieux, et sont souvent accompagnés de communiqués. Quant aux attentats anti-personnel, ils sont essentiellement de nature prédatrice.

Contrairement aux attentats symboliques, les attentats anti-personnel ne sont pour la plupart pas précédés de mise en garde. Ils sont perpétrés dans le but de mutiler et de tuer. Les attentats anti-personnel sont essentiellement : les attentats qui sont perpétrés dans des lieux publics à grande affluence tels que les bars et les magasins, qui frappent à l'aveuglette et ne visent pas forcément des cibles précises; les attentats aux véhicules piégés visant à détruire leur environnement immédiat sans distinction; les attentats perpétrés à l'aide d'engins explosifs à fragmentation qui contiennent des matériaux durs (clous, morceaux de verre, vis, etc.); les attentats utilisant un dispositif explosif secondaire. Ces derniers visent spécifiquement à blesser les premiers répondants (policiers, ambulanciers, pompiers) qui sont dépêchés sur une scène d'attentat à la bombe.

1.4.1.2 **Types d'engins explosifs utilisés**

Les engins explosifs utilisés par les terroristes pour causer la mort, des dommages corporels et matériels sont multiples. Leur utilisation dépend de facteurs tels que la cible à atteindre, les dégâts désirés, la disponibilité de certains matériaux et le savoir-faire des terroristes La conception et l'utilisation d'engins explosifs permettraient de distinguer le niveau de maîtrise technique des organisations terroristes. Certains terroristes ont recours à des engins explosifs artisanaux, dont la puissance peut être variable. Ils sont faciles à confectionner et peuvent être conçus avec des produits commerciaux. Les bombes incendiaires ainsi que les tuyaux explosifs (*pipe bombs*) constituent de bons exemples. Les tuyaux explosifs sont fabriqués à partir d'un tuyau de plomberie, d'un ingrédient actif (poudre noire, poudre de souffre, etc.) et d'un détonateur. Sa fabrication n'exige pas un niveau de connaissance élevé. Sans créer une large étendue du sinistre, ils permettent tout de même de semer l'émoi au sein de la population, L'information (*step-by-step*) permettant de fabriquer ces engins est facilement accessible. En effet, plus d'une centaine de sites sur le réseau Internet divulguent des informations permettant de fabriquer des engins artisanaux. On retrouve aussi une série de publications plus ou moins *underground* consacrées à la fabrication d'engins artisanaux.

Dans d'autres cas, les engins explosifs utilisés par les terroristes ont un niveau de sophistication plus élevé. Ils peuvent être constitués d'un matériel explosif d'origine militaire ou commerciale qui a été volé ou encore fourni clandestinement par un État. Les terroristes les plus avancés au niveau du savoir-faire utilisent des explosifs de plastique tels le *semtex* ou son dérivé le *C-4.* On retrouve près de 27 sortes d'explosifs de plastique manufacturés à travers le monde sous diverses appellations. Ces explosifs sont principalement employés dans la démolition de bâtiments, le minage et servent aussi d'explosif de base dans certaines roquettes et petits missiles. L'explosif de plastique est l'arme de choix des auteurs d'attentats terroristes en raison de ses propriétés: il explose rarement de façon accidentelle; il est malléable; il est difficile à repérer par les appareils à rayons X et par les détecteurs chimiques électroniques; sa texture est élastique et adhésive; une petite quantité suffit pour occasionner des dégâts importants; et il est possible de diriger sa force explosive, Les explosifs de plastique ont été utilisés dans plusieurs attentats.

1.4.2 **Assassinats**

Aujourd'hui, l'assassinat est utilisé fréquemment dans le milieu du crime organisé, principalement chez les organisations criminelles (bandes de motards criminalisés, mafias, etc.) impliquées dans le trafic de stupéfiants. L'assassinat est un instrument de lutte de pouvoir et de règlements de compte. Dans bien des cas, on peut considérer l'assassinat comme un comportement d'auto-justice. Un assassinat peut aussi être l'œuvre d'individus dérangés mentalement. Il existe plusieurs cas d'assassinats de ce genre. Ces assassinats n'ont pas de motif politique, mais sont l'œuvre d'individus au motif obscur ou qui souffrent de troubles psychiatriques.

La tentative d'assassinat du président Ronald Reagan par un «fou furieux » en 1981 en est un bon exemple. Le président américain avait été atteint par un projectile à Washington à l'initiative d'un déséquilibré, du nom de John *Warnock Hinckley,* qui désirait impressionner la comédienne Jodie Foster. Outre les organisations criminelles et les personnes souffrant de troubles psychiatriques, les terroristes ont aussi recours à l'assassinat, dans un but subversif.

L'assassinat peut être définit, comme« *a sneak attacks on defenseless persons who have not offered the assaillant a personal offense*». Bien entendu, l'assassinat est caractérisé par sa préméditation. Il peut se faire techniquement de diverses façons, par l'usage d'explosifs, d'armes à feu, d'armes blanches ou encore à main nue. Le plus souvent les terroristes utilisent des armes à feu, lesquelles permettent de tirer sur la cible à bout portant. Les armes à feu permettent aux terroristes d'être

dissimulés et de tirer à une bonne distance ou servent d'arme de contact, de la même façon que l'arme blanche, en permettant de tirer sur la cible à courte distance dans le torse ou la tête. Il existe plusieurs cas d'assassinats à l'arme à feu. On se souvient, par exemple, de l'assassinat perpétré par l'IRA provisoire, en juillet 1993, contre six membres des forces de sécurité. Les terroristes avaient utilisé, dans ce cas, une carabine *Barrett Modèle 82*, arme qui permet de tirer à plus d'un *mile* et percer un gilet *pare-balle*. Un second exemple est l'assassinat du président égyptien Anouar al-Sadate, le 6 octobre 1981. Ce dernier fut assassiné durant une parade militaire par quatre individus vêtus d'uniformes militaires qui bondirent d'un véhicule du cortège et attaquèrent, à coup d'armes automatiques et de grenades à main, l'estrade où se trouvait Sadate.

Mais l'assassinat peut se produire différemment. Il peut constituer l'aboutissement tragique d'un enlèvement avec séquestration, comme ce fut le cas du ministre du Travail, Pierre Laporte, enlevé par une cellule du FLQ et retrouvé mort dans le coffre arrière d'une voiture à l'aéroport de St-Hubert.

Il existe une autre forme d'assassinat employée par les terroristes. Il s'agit de l'assassinat collectif. Sa logique est différente. Il ne vise pas à éliminer une cible particulière. Le plus souvent les assassinats collectifs sont l'œuvre d'individus qui vont investir des villages de nuit et tuer des personnes, souvent sans considération d'âge ou de sexe. Ils procèdent à l'aide d'armes à feu, d'armes blanches ou encore par le feu. On peut donner comme exemple l'assassinat en Algérie.

1.4.3 Prises d'otages

La prise d'otage constitue une autre méthode qui a été couramment utilisée par les terroristes. La prise d'otage peut prendre deux formes : l'enlèvement avec séquestration et la prise d'otage avec barricade.

1.4.3.1 L'enlèvement avec séquestration

L'enlèvement avec séquestration constitue une vieille méthode utilisée par les malfaiteurs pour extorquer de l'argent. Dans le domaine du terrorisme, les précurseurs des enlèvements avec séquestration sont les Tupamaros d'Uruguay. Ceux-ci ont fait de l'enlèvement de personnalités publiques une arme de revendication politique. L'enlèvement à la Tupamaros a inspiré plusieurs organisations terroristes, dont les Brigades rouges en Italie et le FLQ en 1970. On se souvient d'incidents célèbres, dont l'enlèvement d'Aldo Moro le 16 mars 1978 par les Brigades rouges. Cette

forme de prise d'otage a constitué une source de fonds importante pour certaines organisations terroristes.

L'enlèvement avec séquestration consiste à capturer une personne, ou plusieurs personnes, à en assurer le déplacement et la détention forcée dans un endroit clandestin. Le but de cette prise d'otage est d'obtenir par le chantage l'exécution d'une requête, qui peut être une demande d'argent et/ou une rançon politique, en échange de la libération de ou des otages détenus illégalement.

1.4.3.2 La prise d'otage avec barricade

Les prises d'otage avec barricade peuvent être perpétrées dans divers contextes et avec diverses intentions. Le FBI a regroupé ces prises d'otage dans quatre grandes catégories: la prise d'otage en contexte carcéral, la prise d'otage avec une intention purement criminelle, la prise d'otage perpétrée par des déséquilibrés et la prise d'otage terroriste.

Les prises d'otage avec barricade se produisent autant au sol que dans les airs. Lorsque la prise d'otage implique l'utilisation d'un avion de ligne, on parle de prise d'otage aérienne. Dans ce cas, un groupe d'individus s'empare du véhicule, de son personnel et ses voyageurs pour satisfaire certaines conditions.

1.5 Le cyber-terrorisme

Depuis le 11 Septembre 2001, les pays largement informatisés ont commencé à prendre sérieusement en compte les risques de cyber-terrorisme contre leurs entreprises et leur société en général. Mais il ne faut pas oublier que le cyber-terrorisme, même s'il semble actuellement entrer dans une nouvelle phase d'expansion, n'est pas un phénomène nouveau.
Avec une culture de la connectivité ancrée de plus en plus profondément dans les sociétés dites "modernes", il est promis à un bel avenir. Aujourd'hui, on ne saurait plus vivre sans certains services dont l'épine dorsale est constituée par des réseaux informatiques qui pourraient être réduits à néant par quelques attaques bien réelles, judicieusement menées dans le monde virtuel.

1.5.1 Qu'est-ce que le cyber-terrorisme ?

Le cyber-terrorisme est la convergence entre le terrorisme traditionnel et les réseaux, à commencer par Internet. On peut donc définir le cyber-terrorisme comme l'action délibérée de destruction, dégradation ou modification de données, de flux d'informations ou de systèmes informatiques vitaux d'Etats ou d'entreprises cruciales au bon fonctionnement d'un pays, dans un but de dommages et/ou de retentissement maximum, pour des raisons politiques, religieuses ou idéologiques. Ces dommages peuvent être économiques, sociaux, environnementaux, et même vitaux pour les individus dans certains cas.

Il faut absolument distinguer le cyber-terrorisme du simple cyber-crime, qui consiste à détourner l'usage d'un système dans un but simplement crapuleux.

Pourquoi le cyber-terrorisme est-il destiné à avoir autant de succès ? Pour plusieurs raisons.

Tout d'abord, le coût d'accès est très faible : un ordinateur portable est beaucoup moins cher qu'un explosif brisant ou qu'une arme de guerre. Ensuite, nos sociétés devenant de plus en plus dépendantes des réseaux d'information, la disparition de ceux-ci peut provoquer des effets économiques, logistiques et émotionnels considérables (voir plus loin). De plus, le public et les journalistes sont fascinés par tous les types d'attaques informatiques, ce qui conduit à une large couverture dans les médias. Enfin, la paralysie des pays dits "développés" lorsqu'ils sont privés de réseaux peut faire la part belle aux pays moins équipés et moins vulnérables de ce côté.

1.5.2 Qui sont les cyber-terroristes ?

On distingue en général 3 types de cyber-terroristes.

Les cyber-terroristes sont en général des sous-groupes de groupes terroristes traditionnels. Ces sous-groupes peuvent être non structurés et constitués d'individus peu nombreux, travaillant sans organisation particulière, avec peu de moyens, de préparation, de compétences et de stratégie, ou bien au contraire être parfaitement organisés, avec des moyens conséquents et une définition précise de leurs cibles et de leur tactique. Mais on trouve aussi parmi les cyber-terroristes des sympathisants de groupes terroristes, ainsi que des *hackers* "patriotes", qui vont procéder à des actions de rétorsion juste après des attaques "physiques" (réelles) ou logiques (sur les réseaux) de ceux qu'ils considèrent comme leurs ennemis . En effet, le terrorisme et l'anti-terrorisme s'emparent d'Internet. Ainsi, tout un chacun peut maintenant faire de l'anti-terrorisme de sa propre initiative, sur une base individuelle, pour le plaisir de se faire peur.

Cibles et impacts

Les cyber-attentats avaient pour but de causer un maximum de dommages et/ou un maximum de retentissement médiatique, culturel ou social. La simple défiguration ("effacement") de sites Web peu importants constitue donc à peine le premier niveau des cyber-attentats. Ceux-ci consisteront plutôt à faire tomber des sites critiques ou de grande visibilité, ou à rendre inopérantes les infrastructures critiques d'un pays ou d'une organisation. On peut aussi considérer la corruption de données vitales comme un cyber attentat, puisque la confusion et la chute de confiance créées seront de nature à porter préjudice à la société. Les cibles des cyber-attentats seront donc constituées prioritairement par :

- Les installations de gestion des télécommunications (centraux téléphoniques, points d'accès GSM, réseaux filaires et non filaires, relais hertziens et satellites)
- Les sites de génération et de distribution d'énergie (centrales nucléaires, thermiques, sites de régulation EDF)
- Les installations de régulation des transports (aéroports, ports, contrôle aérien et maritime, gares ferroviaires et routières, autoroutes, systèmes de régulation des feux rouges des grandes agglomérations)
- Les installations de distribution de produits pétroliers (raffineries, dépôts, réseaux de stations services)
- Les centres de gestion du courrier postal
- Les sites de distribution d'eau (usines de traitement, centres d'analyse, stations d'épuration)
- Les institutions financières et bancaires (bourses nationales, réseau SWIFT, home banking, réseaux de distributeurs de billets)
- Les services d'urgence, de santé et de sécurité publique (police, pompiers, SAMU, hôpitaux)
- Les services gouvernementaux (sécurité sociale, assurance maladie, sites institutionnels)
- Les médias (chaînes de télévision, groupes de presse, fournisseurs de contenus divers)
- Les éléments symboliques d'une société et d'un mode de vie (grande distribution, industries représentatives, ...).

Une attaque sur plusieurs de ces cibles simultanément pourrait avoir un effet dévastateur pour un pays non préparé.

Le moment choisi pour les attaques est également important. Les cyber-terroristes choisiront par exemple de frapper en même temps que des événements politiques ou militaires, ou bien quand

l'attention est dirigée dans une autre direction. Ils profiteront également du moment où les procédures se relâchent et où le personnel de surveillance tombe dans la routine.

C’est surtout en réaction à des attaques terroristes ou contreterroristes que les pirates choisissent de frapper.

Les impacts liés à l'attaque des cibles précédentes peuvent être très variés : économiques (des actions ou une bourse peuvent s'effondrer, des entreprises faire faillite), sociaux (chômage, perte de certaines prestations, perte de son "identité sociale"), environnementaux, vitaux. Dans tous les cas, la confusion et la chute de confiance suivant les attaques seront de nature à porter préjudice à la société en général. Les gênes importantes dans les opérations de la vie courante, qui peuvent aller jusqu'au blocage total de certaines fonctions du pays (distribution de billets, d'essence, de produits frais), constituent des dommages majeurs. Certains dommages peuvent même constituer une menace sur la vie de certains individus :

Ainsi, la mise hors service des systèmes de contrôle de refroidissement des réacteurs d'une centrale nucléaire peut conduire rapidement à un accident radiologique majeur (surtout si la chute automatique des barres de secours a été désactivée), nécessitant l'évacuation d'une zone considérable, avec risque vital à plus ou moins long terme pour la population la plus touchée. De même, un aéroport privé de ses systèmes de contrôle aérien aura beaucoup de mal à éviter des collisions, voire des crashes d'appareils. Enfin, un système de traitement de l'eau victime d'une attaque pourra rendre dangereuse une eau qui n'aura pas été suffisamment chlorée, provoquant potentiellement des épidémies. Le cyber-terrorisme a parfois été qualifié de terrorisme sans mort. Cela pourrait changer à l'avenir.

1.5.3 Les armes des cyber-terroristes

Les cyber-terroristes ont à leur disposition, comme nous l'avons vu dans les paragraphes précédents, plusieurs types d'armes logiques pour accomplir leurs attaques. Ces armes sont de complexité et de portées différentes, et leurs impacts peuvent être plus ou moins forts. Parmi les armes les plus courantes, on trouve:

- Les défigurations de sites *Web* et les "attaques sémantiques", Les attaques sémantiques consistent à changer légèrement le contenu des pages Web afin d'en changer le sens, pour faire passer une idée différente de celle d'origine. Cette modification est difficile à détecter pour le webmaster, contrairement à la défiguration simple qui change complètement l'apparence du site Web.

- Les dénis de service simples (DoS), utilisant soit des vulnérabilités précises du système d'exploitation, soit utilisant des techniques plus génériques comme le *SYN* flood.
- Les dénis de service distribués (DDoS), utilisant un grand nombre de serveurs compromis sur lesquels tournent des programmes "zombies" attendant les instructions de ceux qui les ont implantés et qui les contrôlent à distance. De véritables "DDoSNets", constitués par des zombies capables de dialoguer entre eux (*en peer to peer*) et avec leur point de contrôle, se constituent actuellement, qui permettront de lancer des attaques coordonnées aussi rapides que meurtrières sur des cibles bien précises. A cause de ces DDoSNets, les serveurs non sécurisés de n'importe quelle entreprise peuvent se transformer en armes aux mains de cyber terroristes. De même, les ordinateurs personnels connectés en permanence à Internet par ADSL ou par le câble constituent des cibles privilégiées pour ces DDoSNets, et peuvent, là encore, se transformer en armes.
- Les attaques sur les serveurs DNS et les équipements de routage. Les vulnérabilités des protocoles de routage comme BGP, sensible au poisoning, associées à des attaques sur les root servers DNS, peuvent conduire à une paralysie de certaines parties d'Internet : c'est le phénomène de trou noir, où les informations à destination de certains sites disparaissent complètement. De plus, la majorité des routeurs utilisant l'OS de Cisco (IOS), de nouvelles vulnérabilités mises à jour dans IOS conduiraient à des attaques massives.
- Les vers : *Code Red, Nimda, Lion, Adore, Slammer* ont montré leurs capacités. Certains prétendent même que le ver *Slammer* a infecté Internet en 10 minutes seulement. Heureusement, celui-ci ne comportait pas de charge utile hostile et ne résidait qu'en mémoire. On peut imaginer le résultat d'un ver de ce type qui serait capable de mettre hors service instantanément les serveurs infectés, ou de modifier des informations sur ceux-ci...
- Les intrusions classiques, permettant d'implanter des chevaux de Troie, de récupérer des données sensibles ou de mettre hors service des serveurs internes non accessibles autrement.
- La modification furtive de données, suite à une intrusion ou à l'action d'un ver, qui serait capable de décrédibiliser une entreprise ou une organisation, ou même de faire perdre toute confiance en une institution fondée sur cette confiance, comme par exemple la bourse.
- L'implantation de bombes logiques, qui sont capables de se déclencher selon certains paramètres ou certains événements, et peuvent, là encore, faire tomber toute une série de serveurs en même temps, ou modifier des données critiques au moment opportun et de manière automatique.

1.5.4 Les communications, le recrutement et la formation

Les groupes islamistes se servent d'Internet de manière intensive pour leur recrutement, puis pour la formation et l'endoctrinement de leurs recrues. Les perquisitions menées depuis le 11 septembre 2001 dans les milieux Européens supposés être liés à A Q ont montré qu'ils ont utilisé des sites Web de recrutement de mercenaires, comme le site Qoqaz, par exemple. Les mêmes cassettes vidéo ont été trouvées dans une quinzaine d'appartements perquisitionnés. Ces cassettes de formation et d'endoctrinement sont vendues sur Internet, sur des sites comme Maktabah. De même, des newsgroups et des listes de diffusion spécialisés dans la diffusion de sélections documentaires centrées sur l'Islam intégriste présentent les activités des groupes activistes et terroristes au nom de la liberté d'expression.

Quant aux communications opérationnelles, les cyber-terroristes savent aller chercher leurs instructions sur l'un des nombreux sites Web entretenus par leur organisation (AQ a installé des centres de communication Internet à Lahore, Karashi, dans les villages pakistanais du Baloutchistan, d'autres sites sont installés au Cashemire), ou encore sur des channels IRC secrets ou totalement banalisés et créés temporairement, pour l'occasion. Certains recommandent même d'utiliser des messageries instantanées de type ICQ. La multiplication des cybercafés dans le monde entier, y compris et surtout dans les pays en voie de développement, rend la filature des internautes très aléatoire. Pour un dollar chacun, depuis les cybercafés ou les centres d'affaires des hôtels du monde entier, les cybers terroristes d'une même "cellule-action" peuvent communiquer pendant un quart d'heure en direct, sous un pseudonyme, et s'échanger des informations sensibles relatives à un cyber attentat avant de se volatiliser dans la nature. S'ils le jugent utile, ils peuvent confirmer leurs instructions par des messages chiffrés envoyés depuis des messageries anonymes. Mais à quoi bon alerter, par un contenu chiffré, la vigilance des services censés surveiller le contenu du trafic Internet, alors qu'il est tout aussi simple de cacher des messages en clair dans une image anodine ? Vu le nombre d'images qui transitent quotidiennement sur Internet, il n'y a aucune chance que le moindre message caché soit détecté. Point n'est besoin d'utiliser de complexes programmes de stéganographie, utilisant des techniques de masquage élaborées, comme certaines rumeurs en ont fait état. Le texte en clair ou tout juste brouillé est tout simplement ajouté au contenu du fichier image.

1.5.5 L'avenir

Les risques à venir ont de grandes chances de provenir de **DDoSNets de plus en plus élaborés** et de **vers de plus en plus intelligents**, qui vont certainement voir le jour. Des chercheurs ont prédit l'émergence de nouvelles sortes de vers (Warhol worms, flash worms), qui pourraient se diffuser sur Internet en quelques minutes ou même quelques secondes, laissant peu de temps aux administrateurs pour réagir. Des vers hybrides combinant un ensemble de vulnérabilités anciennes, afin de maximiser leurs chances d'infection, ou bien des vers exploitant des vulnérabilités non encore publiées, et donc non pat chables immédiatement, vont certainement voir le jour. De tels vers ne laisseront pas d'autre alternative que de stopper les services en attendant la diffusion du correctif de sécurité par les éditeurs.

Pour l'instant, les vers que nous avons vus passer étaient d'une technologie assez fruste.

Des vers plus sophistiqués et intelligents, pouvant se mettre à jour de manière autonome en allant télécharger des plug-ins plus récents sur des sites précis, pouvant aller chercher de nouvelles cibles et des instructions sur des channels IRC, pourront effectuer des besognes beaucoup plus dangereuses tout en étant beaucoup plus discrets.

1.6 La menace chimique

Le terrorisme par arme chimique ou biologique étant assez difficile à mettre en œuvre, les groupes terroristes classiques préfèrent en général utiliser des moyens de terreur "bon marché" (armes à feu, explosifs, bombes humaines). En effet, les organisations qui peuvent s'en servir avec efficacité sont celles qui ont recruté des scientifiques de haut niveau maîtrisant les sciences biologiques.

1.6.1 Liste de produits biologiques dont les terroristes peuvent se servir :

(Le **bacille du charbon**, la ricine ,la toxine botulique ,la peste (on trouve encore aujourd'hui des épidémies) et **les produits chimiques** : (le sarin ,le soman ,le VX ,le tabun ,l'ypérite)

1.6.2 Comment le groupe terroriste prépare son attaque chimique :

-arriver à se procurer des prélèvements du virus (soit "légalement", c'est-à-dire auprès de distributeurs officiels, soit par vol au sein d'une installation militaire ou d'un laboratoire universitaire par exemple) ;

-installer le matériel ;

-préparer les modes de dispersion adéquats (en fonction du système de ventilation du métro par exemple) ;

-s'occuper du stockage

1.6.3 Comment faire pour que l'agent chimique se disperse le plus largement possible :

-la contamination (par les aliments, l'eau courante)

-l'épandage (par aérosol)

-l'explosion (à partir d'une bombe)

1.6.4 Dans quels endroits utiliser l'arme chimique ?

Principalement dans les lieux "fermés" (stations de métro, gymnases...)

1.6.5 L'empoisonnement collectif par l'eau courante

L'eau est un vecteur privilégié pour contaminer la population à une grande échelle. Cependant, le résultat reste assez improbable car l'eau des réservoirs est filtrée et chlorée. De plus, cette eau est utilisée petit à petit par les consommateurs et l'effet en sera donc limité.

1.6.6 Mars 1995 à Tokyo, Japon - l'action de la secte Aun

Plusieurs groupes de la secte "aun" se répandent dans le métro de Tokyo avec des sacs contenant du gaz **sarin**. Résultat : douze morts et plus de 5 500 blessés. On retrouvera dans les locaux de la secte des produits chimiques entrant dans la fabrication du **sarin** ,

1.7 Après les attentats du 11 septembre 2001

Le 11 Septembre 2001, les Etats-Unis ont été l'objet de quatre attentats au moyen d'avions détournés après leur décollage ; d'aéroports américains : deux ont explosé dans les tours jumelles du World Trade Center, un dans le Pentagone, et un autre en Pennsylvanie. Ce dernier a échoué en raison de la résistance des passagers, l'avion ayant finalement explosé sans atteindre son objectif. Ces attentats ont fait près de six mille disparus dont une majorité de morts. Dans leur tentative de secourir les victimes dès les premières heures, quatre centaines de pompiers y auraient aussi laissé leur vie.

Environ un mois après ces événements (le 7 Octobre 2001), au moment où les Etats-Unis s'engageaient dans une riposte armée contre les *Talibans* notamment le réseau (AQ) de Oussama Ben Laden (OBL), accusé par l'administration Bush, d'être à l'origine de ces attentats, une vague bio terroriste a fait son apparition : des lettres contenant de l'anthrax sont envoyées à des institutions fédérales et à certaines personnalités américaines aussi bien aux Etats-Unis, qu'en dehors. Le réseau d' (OBL) est soupçonné d'être à l'origine de ce terrorisme biologique. Toutefois, selon les dernières informations, il semblerait que ce volet de la crise actuelle serait plutôt de la responsabilité de groupes extrémistes américains ou l'œuvre d'un scientifique militaire américain qui compte ainsi relancer et accroître le financement de ses recherches liées à l'anthrax ! D'autres sources estiment qu'il pourrait s'agir de responsabilités irakiennes, mais des scientifiques américains affirment que des composants présents dans la poudre ne peuvent être produits que par les Etats-Unis ou la Fédération de Russie. En d'autres termes, l'origine de ce bioterrorisme reste encore incertaine. Il faut juste souligner que, dans tous les cas, le bioterrorisme à l'anthrax n'est pas une nouveauté pour les Américains qui, depuis des années déjà, vivent sous cette menace : des personnes ayant des liens forts avec l'extrême droite ont déjà été arrêtées pour avoir été à l'origine de tentatives de contamination à l'anthrax durant les dix dernières années. L'échafaudage apparemment sûr des sources possibles permet à l'administration de rassurer la population en lui donnant l'impression qu'elle contrôle la situation, alors même que les responsables du *Federal Bureau of Investigation* (FBI) font état de réelles impasses dans les enquêtes.

Cette crise dont a le terrorisme est le noyau dur, a un impact important sur les relations internationales aujourd'hui, et doit être appréciée dans une optique prospective afin de déterminer les moyens pour l'humanité d'échapper à son autodestruction.

1.7.1 Conséquences dans les rapports internationaux.

1.7.1.1 Une remise en cause de l'uni polarité

Depuis la fin de la guerre froide, il était convenu qu'il ne restait qu'une seule puissance, les Etats-Unis. L'aptitude de l'Europe des Quinze, de la Chine ou de la Fédération de Russie à concurrencer la puissance américaine et à mettre fin à cette hégémonie reste discutée. Avec les attentats du 11 septembre, la menace contre la puissance nous amène à relativiser cette hégémonie, même si les discours politiques internationaux n'en ont pas fait état. Cette menace qui a frappé le puissant n'épargne personne : c'est une puissance diffuse qui choisit ses cibles selon une logique qui n'est pas perceptible et rationalisable.

Cette menace nouvelle par la dimension qu'elle a prise, identique pour tous – puissants et faibles – et diffuse, conduit forcément à reconsidérer l'uni polarité. En réalité, la menace constitue aussi un pôle de puissance qu'affronte la coalition anti-terroriste sous la houlette des Américains. Car dans une situation d'hégémonie, la puissance a tendance à imposer ses intérêts ; tandis qu'avec cette menace diffuse, il paraît plus « tactique » de ne point agir en puissance. Indirectement ; une forme de morale s'introduirait dans les relations entre les Etats, puisque les puissances devront prendre en compte d'autres intérêts comme ceux des Etats plus faibles. Mais il ne faut pas ignorer un autre risque de cette évolution, qui est l'instrumentalisation des intérêts des Etats faibles : ceci conduirait à la situation antérieure, de sorte qu'elle ne peut que raviver les menaces.

Cette menace et cette tolérance appellent un nouvel ordre international dont il est question depuis fort longtemps, et qui n'est toujours pas, car c'est une nouvelle ère où le fort reste aussi faible face à une menace aveugle, mondiale et diffuse. Certes l'expression a été galvaudée, et les diplomates aux Nations Unies l'ont souvent utilisée comme une incantation notamment s'agissant des questions de droit international du développement. Il n'empêche qu'il faut une nouvelle forme de relations internationales différente des situations de domination directe ou indirecte, qui assure un réel développement, c'est-à-dire « l'épanouissement de la personne dans ses dimensions individuelles et collectives, dans le respect des intérêts de la communauté internationale et des générations futures ». Ce nouvel ordre doit cependant être distingué de l'idée de contrat mondial ou d'une plus grande implication du secteur privé, dont a pu parler l'actuel Secrétaire général. Car dans cette dernière proposition il y a une logique commerciale de profit qui risque de l'emporter sur la nécessité de relations internationales plus équitables.

Ce nouvel ordre se fondera aussi sur une stratégie internationale nouvelle basée sur une menace commune : le terrorisme. Tous les Etats ont un même intérêt à le combattre en collaborant pour la

sécurité internationale. Car nul n'est à l'abri de tels actes terroristes. L'intérêt particulier d'aucun Etat ne saurait l'emporter trop souvent dans les relations internationales : les Américains ont tendance à faire primer leurs intérêts économique, militaire et stratégique sur ceux de tout le monde. Désormais il ne devrait plus en être ainsi.

1.7.1.2 Une nouvelle remise en cause de la politique étrangère des Etats-Unis

Ces attentats induisent une remise en cause de la politique étrangère des Etats-Unis, même si leurs réactions ne laissent pas percevoir cette lecture des faits, d'autant plus que la réaction américaine aux attentats du 11 septembre peut produire une dynamique dont les acteurs n'ont pas conscience.

Jusqu'à présent les Etats-Unis ont adopté une stratégie de politique internationale du « chien de garde » : recourir à un Etat de la région pour contenir toute menace régionale. Or ce « chien de garde » finit par être « enragé » et, à terme, constitue lui-même une menace. C'est ce qui était advenu avec l'Irak de Saddam Hussein : d'abord allié des Américains contre l'Iran, aujourd'hui ennemi public américain. Avec les *Talibans* et OBL, l'histoire n'est pas différente.

Au lieu d'en tirer les leçons comme il se doit, les Etats-Unis se reposent aujourd'hui sur le Pakistan et l'Ouzbékistan. Et contrairement à certaines expectatives sur une meilleure coopération entre les Etats pour lutter contre la puissance désormais diffuse – mais autrefois étatique – du terrorisme international, les Etats-Unis font quasiment cavalier seul et n'associent la communauté internationale que pour asseoir leur légitimité, la légalité restant difficile à acquérir en l'espèce, en ignorant les mécanismes internationaux de règlement des différends.

L'ONU n'est pas vraiment redevenue cette assemblée où tous les Etats élaborent un plan d'action sur la base du principe de l'égalité des Etats, car elle n'est qu'informée des opérations et n'y participe pas tout à fait. Certes elle tente de mettre en place une stratégie post-talibane, mais ce processus post-conflictuel est soumis à la volonté des parties afghanes et aux vicissitudes des luttes entre différents groupes. Le fait que les Etats-Unis soient les premiers en ligne de mire, ayant été victime des attentats, ne facilite pas non plus l'action multilatérale, et constitue un facteur paralysant pour le mécanisme onusien. Car les Etats-Unis feront obstruction toutes les fois où cette action n'irait pas dans le sens de leur choix. Ce qui n'est qu'une pure leçon de réalisme politique, de toute évidence, ce ne sont pas des mécanismes juridiques qui garantissent la sécurité internationale ; ils ne peuvent agir que dans des situations politiques où règne un minimum de consensus sur le degré insupportable de la violence. On pourrait ainsi se demander pourquoi après les attentats de Naïrobi, de Dar es-Salaam et d'Oman, il n'y a pas eu une telle levée de boucliers contre le terrorisme ? Ce

qui a changé ; c'est la prise de conscience qu'il n'y a plus de cibles que le terrorisme ne puisse atteindre et la volonté des auteurs des attentats terroristes de faire un maximum de victimes.
Il est souhaitable que les Nations Unies soient plus impliquées, mais elles doivent avoir une position plus « équilibrée » afin d'une part de respecter son statut d'Organisation Internationale non partisane et, d'autre part, d'éviter à l'Organisation d'être la cible de manifestations hostiles.

1.7.1.3 Un changement dans le règlement des conflits du Moyen-Orient

Cette crise présente aussi une grille de lecture spéciale s'agissant des conflits au Moyen-Orient, notamment de la question palestinienne. AQ, par la voix de son président, OBL, n'a pas manqué d'appeler les Etats-Unis à une politique plus « juste » dans le conflit qui oppose Israël et Palestine. Tous les pays du Tiers-Monde posent le débat en ces mêmes termes : pourquoi l'Etat palestinien n'a toujours pas vu le jour contrairement à la même résolution qui a justifié la création d'Israël ? Résoudre la question israélo-palestinienne prend une telle importance pour les Américains qui cherchaient à se sortir de ce « bourbier diplomatique », car en la liant aux attentats, OBL et son réseau ont enchaîné les Etats-Unis à obtenir des résultats concrets. La paix en Palestine devient quasiment un objectif de politique intérieure, puisqu'en dépend la sécurité des citoyens américains. Or cette paix ne peut pas se faire autrement que par des concessions importantes de l'Etat d'Israël.

1.7.1.4 Une analyse critique de l'action militaire américaine

Les chances de succès de l'action américaine contre OBL restent *a priori* nulles !
La riposte américaine a certes permis la victoire militaire de l'Alliance du Nord soutenue par un armement russe renouvelé, mais est-ce pour autant que l'objectif initial d'atteindre OBL et d'éradiquer le terrorisme sera atteint, le doute demeure et pour longtemps encore peut-être. Car même si OBL est atteint physiquement, directement ou indirectement, le terrorisme ne risque pas de disparaître, parce que d'une part les tentatives de vengeance de ses fidèles ne manqueront pas, et d'autre part parce que les OBL pullulent et n'attendent que le moment où ils pourront frapper. Ainsi qu'a pu le dire M. Nelson Mandela, « toute action [militaire et totale] serait aussi impopulaire que celle des terroristes ». Pire, ces clones potentiels d'OBL ne sont pas souvent bien loin, sous la juridiction d'Etats conciliants ou incapables… Ils sont bien des fois au milieu même de la société qu'ils combattent, aux Etats-Unis ou partout en Europe. Il est donc clair que des bombes sur l'Afghanistan, sur l'Irak, la Somalie, ne constitueront pas des solutions à long terme contre le terrorisme. Enfin il est difficile de croire que les causes à l'origine du terrorisme disparaîtraient aussi

aisément. Car il ne faut pas oublier que la définition du terrorisme reste sujette à caution même si la distinction entre les terrorismes national et international paraît établie et que toute opposition armée de pouvoirs établis a pu être qualifiée de terroriste.

AQ est un réseau de mouvements terroristes dont la plupart sont inscrits sur la liste noire des Etats-Unis. Une véritable contre-offensive pour éliminer AQ comme le prétendent les autorités américaines, implique non seulement l'opération armée actuelle sur l'Afghanistan, mais aussi dans d'autres pays du monde (partout où résident les composants de ces mouvements) : la même difficulté de mise en œuvre de l'opération apparaît encore, et la nécessité d'une coalition internationale autre que l' actuelle s'impose pour que chaque Etat procède à l'élimination des mouvements terroristes dans les territoires sous sa souveraineté.

1.7.1.5 Des relations interreligieuses plus difficiles

Enfin cette crise va accentuer les difficultés sociales que rencontrent nombre de pays avec leurs communautés musulmanes. Ainsi aux Etats-Unis mêmes, une école islamique a été brûlée dans le Kentucky et les étrangers, surtout ceux que les forces de l'ordre (notamment la police des frontières) identifient comme étant d'origine arabe, sont l'objet de mesures de sécurité particulières. Aux Kenya par contre, ce sont des églises qui ont été brûlées par des islamistes, en réaction contre l'opération militaire de la « communauté internationale christianisante ». Au Nigeria, les brutalités contre les populations chrétiennes dans les Etats islamiques du Nord se sont accentuées. Au Pakistan, des violences similaires sont à souligner notamment à Quetta.

Contrairement aux prédictions, il n'est pas possible qu'il s'agisse d'un conflit civilisationnel. OBL et les mouvements terroristes ne constituent pas une civilisation, D'ailleurs lorsqu'ils bénéficiaient du soutien américain, ils n'étaient point considérés comme une civilisation ou une culture rivale ou opposée. Il est inutile de revêtir la lutte contre ce terrorisme d'une vision manichéenne : du Bien contre le Mal, de l'islam contre la chrétienté ou de l'orient contre l'occident. C'est fausser l'analyse en lui ôtant toute objectivité et exposer les populations à la menace de l'intolérance et de la vengeance.

Il revient aux Nations Unies de faire entendre un tel discours unificateur, en rectification d'erreurs que véhiculent les discours des terroristes et auxquelles certains citoyens du monde sont sensibles à défaut d'entendre mieux. D'ailleurs le secrétaire général de la Ligue arabe a affirmé le dimanche 4 novembre 2001, que OBL ne parle point au nom des musulmans, ni au nom des Arabes.

1.7.2 Conséquences économiques

L'impact économique du 11 septembre ne saurait être contesté dans la mesure où les attentats ont touché le cœur même de l'économie américaine et, par voie de conséquence, internationale. Toutefois il est important de souligner que les analyses sur l'économie américaine ont évolué récemment. Ainsi les experts économiques américains reconnaissent que la récession américaine actuelle a commencé, et que contrairement à nombre d'affirmations politiques, elle ne résulte pas principalement des attentats du *World Trade Center* et du Pentagone. En gardant cela à l'esprit, ont des répercussions sur le transport aérien, le tourisme et pour les banques.

1.7.2.1 Sur le transport aérien

Le transport aérien est particulièrement touché par les événements du 11 septembre, parce que ce fut le vecteur des attentats, sans compter que les avions ont connu aussi un certain nombre de déconvenues indépendantes des développements actuels. Les compagnies aériennes voient leurs difficultés financières aggravées par cette crise. C'est le cas des compagnies nationales comme Sabena et *Swiss Air* qui ont déposé le bilan. La Lufthansa aussi se prépare à devoir en faire de même.

1.7.2.2 Sur le commerce du tourisme international

Le transport aérien touché, l'industrie du tourisme n'est pas en reste. Les deux marchés sont liés. Toutefois, il faut se garder de toute conclusion hâtive car la période n'est pas particulièrement propice au tourisme international : seules des analyses à long terme pourront confirmer que les taux décroissants actuels sont une conséquence des attentats. Déjà la presse se fait l'écho d'une crise profonde dans le tourisme.

1.7.2.3 Sur les relations bancaires internationales

En matière bancaire, les relations sont d'un type particulier. Car le système bancaire international a été utilisé par les terroristes dans la mise au point de leur stratégie. En conséquence, il est nécessaire de pouvoir retracer le parcours des fonds ayant contribué à la réalisation des attentats. Or le secret bancaire reste un frein. Les paradis fiscaux ont servi l'argent du terrorisme, et l'objectif actuel des gouvernements partis à la coalition antiterroriste est de lever l'opacité légendaire des flux financiers

internationaux. La dénonciation des paradis fiscaux protégés par la Couronne, notamment les Iles Vierges, Cook et Caïmans, mais aussi par la France comme Monaco, et la Suisse elle-même, s'impose et est récurrente dans la presse internationale. Cette dénonciation s'est faite aussi dans l'arène politique, certains parlements ayant publié des rapports à cet égard.

S'agissant plus particulièrement de l'Afrique, il ne ressort pas des études du GAFI (groupe d'action financière contre le blanchiment des capitaux mis en place dans le cadre de l'OCDE), que les Etats africains soient particulièrement moins coopératifs et plus opaques que sur d'autres continents.

1.7.3 Conséquences juridiques

Des conséquences quant à la normativité internationale, sont aussi à prévoir même si elles n'apparaissent pas encore. Et elles se situent d'une part dans la dimension coutumière de certaines règles du droit international notamment la légitime défense et la mise hors-la-loi du recours à la force. De même, la pratique des dommages collatéraux se perpétue au risque de constituer une coutume limitant les deux principes majeurs du droit international humanitaire : principes de nécessité et de discrimination. Le hangar de la Croix-Rouge à Kaboul aurait été touché à deux reprises. Dans le même ordre d'idées des erreurs de frappes militaires, les bombardiers américains ont touché, selon la presse française, une colonne de blindés de l'Alliance du Nord. Mais sur la dimension humanitaire, c'est-à-dire de l'action humanitaire, de l'assistance aux populations en danger, il faut souligner que la prise en compte immédiate de l'intérêt des Afghans est à mettre au crédit des Nations Unies et des Etats qui ont milité en ce sens. Toutefois il serait plus efficace d'instituer une contractualisation souple, courte et donc révisable, suivant le principe d'une co-responsabilisation des acteurs.

Quant aux normes relatives au terrorisme, il faut se demander s'il est nécessaire de déterminer de nouvelles règles afin de mieux combattre ce fléau. Pour notre part, trop de droit tue le droit. Il serait impératif d'appliquer les nombreux textes actuels qui offrent déjà un cadre juridique large pour l'appréhension des actes terroristes. Si ces textes ne sont pas encore entrés en vigueur, il suffirait que les Etats fassent preuve d'une plus grande bonne volonté pour qu'il en soit ainsi, et que ces textes connaissent leur pleine application. Privilégier le cadre international constitue aussi une réponse à la dimension extraterritoriale de la législation américaine en la matière.

Deuxième partie
Les sources du financement d'activités terroristes

Dans cette deuxième partie, je vais décrire les différentes sources de financement ainsi que les modes d'opérations des différents groupes de transferts de fonds et le blanchement et financement d'activités terroristes.

2.1 Différentes sources de financement d'activités terroristes

Pour mettre à jour les différentes formes que revêt l'infrastructure financière des groupes terroristes, nous devons étudier des documents et d'analyses. En dépit des informations abondantes dont les sites Internet font état et qui sont disponibles au grand public, une constante demeure: certaines activités sont légales, d'autres sont illégales, et un nombre important se trouvent dans une zone grise où la légalité fluctue ou reste ambiguë; l'identification des participants n'est pas une chose aisée; les destinataires des fonds ne sont pas systématiquement connus; l'utilisation des fonds est mixte, par exemple, à la fois pour des œuvres caritatives et pour des fins terroristes. À cela s'ajoute la possibilité que des membres de l'organisation détournent pour des fins personnelles des fonds destinés à des activités terroristes.

2.1.1 Source de financement d'activités terroristes :

- Étatiques (états dévoyés-états escroqués-états en contexte de conflit armé)

- À légalité variable (don de particuliers-organismes humanitaires-cotisations-vente de

publication/marchandises).

- Illégales (activités criminelles organisées- enlèvements- extorsions -contrebande-fraudes - soutien financier des militants et des diasporas (L' E.T.A au pays Basque ou l'I.R.A en Irlande) - l'impôt révolutionnaire, qui prend en fait la forme de racket organisé, essentiellement auprès des entreprises (les sociétés d'import-export sont très pratiques pour les mouvements de fonds et de matériel par exemple).

2.1.1.1 Le financement par l'État

Une source de financement des activités terroristes est attribuée à l'apport et au soutien explicite d'États qui contribuent à fournir les fonds, les armes et le matériel technique nécessaire aux actes projetés. Selon le Groupe d'action financière sur le blanchiment de capitaux, ce terrorisme « sous l'égide des États » serait en déclin. Quoi qu'il en soit, cette source de financement reste importante, dans la mesure où elle pourrait toujours resurgir ou s'intensifier si des événements politiques majeurs en mesure de bouleverser l'ordre mondial devaient survenir.

2.1.1.2 Les sources à légalité variable ou ambiguë

Estime crucial de faire la différence, les sources de financement légales qui proviennent de la même région géographique que celle où se commettent les activités terroristes, et celles qui viennent de pays différents. Cette précision est effectivement féconde. Le Canada, par exemple, est en général considéré comme une « terre d'accueil » pour les terroristes qui procèdent à des activités variées de financement sur son territoire, dont les fruits seraient ensuite envoyés soit par le réseau bancaire officiel, soit par les systèmes informels de transfert des fonds, En l'occurrence, il importe de relever les distinctions entre les activités de financement opérées dans un pays où des actes terroristes ne seront pas commis et les activités de financement perpétrées dans un pays où des actes terroristes se produisent.

— Les dons et le financement en provenance de particuliers:

Des individus fortunés appartenant ou non à une organisation terroriste sont partie prenante au financement d'activités terroristes, en contribuant aux dépenses encourues par le groupe supporté.

— Lever directement des capitaux par le biais d'activités « génératrices de revenus ».

Les terroristes peuvent « tirer une partie de leurs ressources de revenus perçus de façon légitime ». Il importe aussi de prendre en considération que des sources de revenus proviennent d'entreprises commerciales légitimes: les groupes terroristes « obtiennent aussi des dons de chefs d'entreprise compréhensifs ».

— Les revenus en provenance d'organismes humanitaires et d'associations de charité:

Les membres d'une communauté, en raison de leurs croyances religieuses, sont invités à donner une partie de leurs revenus à des fins d'éducation, de soins de santé, ou en vue de l'achat de médicaments. Dans ces cas une partie des capitaux recueillis à des fins humanitaires est détournée pour des activités terroristes. En fait, les organismes religieux et de secours font partie d'une catégorie plus vaste d'organismes à but non lucratif. Les formes de ces organismes sont multiples et sont susceptibles de s'adapter aux pays et aux régions où ils s'installent pour des motifs pluriels. On relève ainsi: les associations, fondations, comités de collectes de fonds, organismes de services locaux, entreprises d'intérêt public, organismes constitués en sociétés anonymes et institutions publiques de bienfaisance, Les motifs de collectes de fonds de ces organismes sont variés:

Caritatifs, religieux, culturels, éducatifs, sociaux ou confraternels, et autres bonnes œuvres.

En matière de financement d'activités terroristes, il n'est pas toujours possible de distinguer entre les organismes à but lucratifs ou non lucratifs qui sont utilisés à leur insu par les terroristes et ceux qui sont établis précisément à cet effet. *La collecte de cotisations et/ou de frais d'inscription*: comme la vente de cartes de membres.

- La vente de publications: comme du matériel de propagande.

- Les tournées de conférences, manifestations culturelles et sociales:

- La sollicitation (porte à porte) auprès de la communauté visée: souvent effrayée par les menaces ou la crainte de représailles, certains membres d'une ethnie en exil est contrainte de contribuer aux causes terroristes. Les contributions peuvent également être volontaires.

- Les revenus en provenance d'associations civiques et confessionnelles: « Depuis le début des années 1990, les groupes terroristes dépendent de plus en plus des dons provenant de ces associations »

2.1.1.3 Les sources illégales

—*Activités criminelles qui s'apparentent à celles d'organisations criminelles*: on peut noter, entre autres le recours au trafic de stupéfiants, et la fausse monnaie. La fausse monnaie constitue le meilleur moyen de financement du trafic de drogue et surtout du terrorisme.

—*Enlèvements ou extorsions*: les rançons payées pour libérer les otages ainsi que les fonds extorqués aux entreprises, l'« impôt révolutionnaire », constituent une importante source de financement pour les terroristes. Ces ressources garantissent une forme de régularité dans les revenus escomptés, en raison des populations captives qui en subissent les effets concrets.

—Activités de contrebande à grande échelle: trafic de diamants, de pierres précieuses

—Différents types de fraud*e*: comme les opérations frauduleuses sur cartes bancaires.

—Formes variées de vols, de cambriolage: par exemple, vols d'automobiles. En outre, le hold-up constitue une autre source de financement déjà utilisée par les terroristes

2.2 Les sources de financement du terrorisme et les modes d'opération d'un groupe

À la suite d'analyses issues de textes récents sur les tendances actuelles du terrorisme il apparaît pertinent d'examiner trois hypothèses:

1- que les modes d'opération des groupes terroristes seraient spécifiques à chacune des organisations étudiées;

2 - que les sources de financement ne sont pas fixées dans le temps et dans l'espace mais au contraire fluctuent et évoluent;

3 - que les groupes terroristes sont susceptibles de privilégier des moyens légaux de financement dans les pays où ils ne commettent pas d'actes terroristes, qui restent ainsi des « zones d'activités secondaires ».

En effet, comme nous l'avons déjà mentionné, pour saisir dans toute sa complexité la question du financement des activités terroristes il faudrait distinguer entre les pays où un groupe commet ses actes terroristes (« zones d'activités primaires ») et les pays où il n'en commet pas et se limite à des activités de support. Pour bien des groupes internationaux. Quelques pays se situent dans la seconde

catégorie : c'est un espace commercial choisi et utilisé en raison de sa position géographique stratégique, où le groupe ne commet pas d'acte terroriste violent et évite ainsi d'éveiller l'attention des autorités. Ainsi, s'y livrer à des activités de financement trop visiblement illégales serait inconséquent. Par contre, plusieurs formes de financement illégales mais hautement efficaces sont utilisées dans des endroits où a) le groupe est déjà ciblé par les autorités) les autorités sont impuissantes devant à la fois le terrorisme et la criminalité.

Il y a également des cas où les activités illégales de financement et les actes terroristes se renforcent mutuellement: les activités illégales de financement permettent la commission d'actes terroristes et, les actes terroristes permettent la poursuite des activités illégales de financement. De fait, attribue directement aux encouragements prodigués par la CIA et L'ISI (les services de renseignement pakistanais) la prolifération de la culture et du commerce de l'opium au cours de la guerre d'Afghanistan de 1979-1989. Ces récoltes devaient servir au financement des combats et affaiblir les forces soviétiques suite à la diffusion de la drogue, ce qui se révéla un héritage encombrant pour les démocraties occidentales. L'autre exemple typique étant celui du soi-disant « narco-terrorisme » d'Amérique Latine, élément majeur de la justification de la « guerre contre la drogue » dans les années 1980.

Un élément crucial de tout terrorisme reste la diffusion massive des actes commis, la recherche d'un maximum de publicité. Il faut donc se demander à quel point, et de quelle manière les groupes terroristes se soucieraient de la manière dont des actes criminels influenceraient leur réputation dans les zones primaires aussi bien que dans les zones secondaires, où ils tentent souvent de présenter une image politiquement acceptable de groupe oppressé.

Aux activités policières et à la gestion des relations publiques s'additionnent un certain nombre d'autres facteurs qui influencent le choix de moyens de financement :

- l'identification avec un espace géopolitique;

- la nécessité d'affirmer la présence du groupe terroriste sur un territoire;

- avoir la capacité de faire fuir la compétition, c'est-à-dire que les organisations criminelles qui voudraient récupérer des trafics prolifiques ne soient pas en mesure de le faire en raison de la crainte de représailles;

4- devoir assurer la cohésion du groupe en se consacrant à des activités organisées.

5- devoir assurer au groupe des sources de revenus continues.

2.3 Les transferts de fonds

2.3.1 Les systèmes informels de transfert de fonds

Dans le but de cerner le phénomène à l'étude et d'en préciser l'ampleur, la portée et l'importance pour les activités de financement du terrorisme, il importe de confronter entre elles les diverses définitions légales, économiques, politiques et culturelles des systèmes informels de transfert de fonds. En effet, la lecture relative à la diffusion, à l'utilité et au maintien de ces modes de transfert de fonds opérant en marge des réseaux bancaires officiels, est susceptible de se modifier selon les éléments contenus dans la définition et les effets recherchés par ceux qui y en précisent les paramètres. De fait, certains auteurs tentent de distinguer entre la lutte mondiale contre le financement du terrorisme et les aspects fondamentaux des systèmes de transfert de fonds. C'est d'ailleurs, la perspective qui est adoptée ici.

2.3.2 Définitions et terminologies : des lectures partielles

Premièrement, le mot « *Hawala* » signifie, à la base, « transfert » et dans certains contextes « confiance », en arabe. Son usage implique que les activités restent informelles et fondées pour l'essentiel sur une relation personnelle entre les participants. . Le Groupe d'action financière sur le blanchiment de capitaux a recours à l'expression « systèmes informels de transfert de capitaux ou de valeurs » (ITCV) pour désigner:

un système dans lequel de l'argent est reçu afin que ces fonds ou leur contre-valeur puissent être payés à un tiers dans un autre lieu, que ce soit ou non sous la même forme. Ce transfert intervient généralement en dehors du système bancaire classique par l'intermédiaire d'institutions financières non bancaires ou d'autres entités commerciales dont l'activité principale peut ne pas être la transmission d'argent. Dans certains pays ou territoires, les systèmes ITCV sont souvent désignés comme des services **alternatifs** de remise de fonds ou des systèmes bancaires souterrains ou encore parallèles.

Pour, « l'*hawala* est un système de transfert de fonds qui ne passe pas par le canal des institutions financières classiques. Ce mode de transfert à donc un caractère **informel** ». Pour leur part, ils parlent de systèmes **non réglementés**. Ils soulignent également le foisonnement des définitions de ces systèmes dans la littérature. Par exemple, certains auteurs les qualifient de « **souterrains** », ce serait une erreur dans la mesure où ces systèmes opèrent à l'air libre dans de nombreuses régions du globe. De plus, avoir recours à l'expression « **système bancaire** » constitue également une voie erronée puisque. Dans le *Patriot Act*, la loi adoptée par les États-Unis pour redéfinir leur mode d'intervention en matière d'activités terroristes, c'est l'expression « *systèmes bancaires souterrains*» qui est utilisée, combinant deux erreurs conceptuelles. D'autres encore ont adopté la terminologie « systèmes **alternatifs** ». Comme le remarquent fort, les systèmes informels de transfert de fonds ne sont pas, dans de nombreux cas, des alternatives au système bancaire officiel, étant donné que ce serait le seul dispositif de transit de fonds disponible au niveau local et régional.

En fait, la principale caractéristique de ces systèmes est leur absence de bureaucratie. Cependant, dans le but de saisir les différents termes en usage dans les écrits gouvernementaux et les diverses agences de surveillance des mouvements bancaires, il importe:

de distinguer le système du terme *hawala* lui-même, qui signifie « transfert » ou « télégramme » dans le jargon bancaire arabe. Dans l'acception retenue ici, l'*hawala* désigne un réseau informel de transfert de fonds d'un lieu à un autre par le biais de courtiers — *les hawaladars* — quelle que soit la nature de la transaction ou les pays impliqués.

En terminant ce tour d'horizon nominal il importe, de distinguer entre l'***hawala* blan**c et l'***hawala* noir**. En effet, les systèmes informels de transfert de fonds peuvent être l'occasion pour d'honnêtes travailleurs de faire circuler de l'argent gagné légalement (*hawala* blanc), comme ils peuvent être récupérés par des organisations criminelles ou par des groupes terroristes pour faire transiter des fonds illégalement obtenus (*hawala* noir) ne manque pas d'intérêt: *« Hawala works by transferring money without actually moving it* ». En fait, l'argent circule sans avoir à se déplacer. Une définition, donc, qui semble appropriée au contexte géopolitique de ces systèmes informels: *« money transfer without money movement ».*

2.3.3 Une continuité séculaire

Les systèmes informels de transfert de fonds, dont le financement *hawala*, sont des modes de transfert d'argent plus que centenaires. Il existe un grand nombre de systèmes informels de transfert de fonds, certains connus, d'autres qui opèrent dans l'invisibilité, dans la mesure où ils ne sont pas repérés par les organismes gouvernementaux et par les instances affiliées à la surveillance internationale du financement d'activités terroristes. Dans le cadre de la discussion actuelle

2.3.4 Des systèmes adaptés à une population émigrante

Lorsque des populations émigrantes ont tenté d'envoyer à leurs familles restées au pays leur salaire gagné à l'étranger, elles se sont tournées tout naturellement vers des méthodes éprouvées que ni le temps, ni les guerres, ni les bouleversements historiques, politiques, culturels et sociaux n'avaient altérés. En fait, les travailleurs émigrés ont adopté les systèmes informels de transfert de fonds non seulement pour des raisons d'économie ou pour des questions de taux de change avantageux, mais surtout parce que ces systèmes correspondaient parfaitement à leurs attentes: un service efficace, rapide, apte à se déployer dans toutes les régions, en osmose avec leur *pattern* de revenus (irrégulier ou régulier, pour des sommes importantes ou pour de plus petites) et basé sur un réseau d'interactions entre des intermédiaires en mesure de mobiliser des modes de transfert de fonds innovateurs .

Pour comprendre l'attrait que représentent les systèmes informels de transfert de fonds pour un grand nombre d'agents économiques inquiets de l'instabilité politique de leur pays ou d'une région en particulier, il faut comprendre que les utilisateurs de ces services y voient la possibilité de bénéficier de services adaptés, rapides, sûrs, et en mesure de leur permettre, dans certains cas, de consolider des évasions fiscales. En outre,

Les participants sont en mesure de capitaliser sur les forces du marché pour pallier aux insuffisances des infrastructures conventionnelles des pays développés et en voie de développement, incapables de répondre aux besoins des populations en exil.

2.3.5 Des liens forts entre les participants

Le système informel de transfert de fonds *hawala* se fait en utilisant de nombreux intermédiaires et opère en ayant recours à un ensemble de devises. De fait, le système dans son ensemble est basé sur la confiance, le respect des traditions, l'amitié, les relations égalitaires, un sentiment d'appartenance

à un ethnie commune, à une communauté culturelle: « de forts liens ethniques, voire familiaux unissent les différents maillons des réseaux de courtiers qui quadrillent le globe » . Le système fonctionne parce que les participants partagent entre eux le même sens de l'honneur. En outre, les représailles qui pourraient survenir contre ceux qui seraient tentés de désobéir aux règles implicites du réseau suffisent à garantir le respect et l'adhésion des membres aux coutumes ancestrales.

2.3.6 Une réponse aux coûts élevés des banques

Pour de nombreux travailleurs et pour les immigrants venus chercher asile et fortune dans les pays riches, « traiter avec des établissements occidentaux comme *Western Union* qui prennent des commissions beaucoup trop élevées » ne constitue pas une option attrayante. Au contraire, un *hawaladar* (courtier) se contentera d'une somme moins importante pour effectuer le transfert de fonds.

2.3.7 Les transferts de fonds et le financement d'activités terroristes

En effet, pour tenir compte des caractéristiques spécifiques à la problématique du terrorisme, il convient de ne pas systématiquement associer le **blanchiment** de capitaux (que l'on attribue volontiers aux organisations criminelles) et la tentative avouée des terroristes de dissimuler le *destinataire* des fonds transmis, soit par des voies officielles (les réseaux bancaires) soit par des systèmes de transfert de fonds informels. Dans le cas du blanchiment d'argent ce n'est pas le mouvement des fonds qui est le motif d'appréhension des infracteurs présumés, mais bien leur source. En fait, ce qui importe et qui sera pris en compte par les autorités policières et judiciaires, c'est le crime ayant produit les fonds et pour lequel il est apparu nécessaire de procéder à une opération visant à donner une légitimité aux sommes d'argent encaissées. Généralement il est question de trafic de drogue, de vente d'armes, etc.

2.3.8 L'attrait des systèmes informels de transfert de fonds : pas de trace de papier

Les systèmes de transfert de fonds fonctionnent **sans interruption** et tous les jours, leur assurant une popularité et une fidélité de la part de leurs utilisateurs. En outre, celui qui envoie l'argent et le destinataire peuvent être une seule et même personne. Dans tous les cas, en évitant les circuits formels de transferts d'argent, le destinataire peut rester **anonyme** et échapper à la surveillance des organes de contrôle. À l'évidence, le principal attrait des systèmes informels de transfert de fonds,

c'est qu'il n'y a pas de moyens de repérer le parcours emprunté par l'argent.. Étant donné qu'il s'agit de transactions aptes à se réaliser avec un minimum de documents écrits.

Les individus ou les groupes terroristes qui optent pour les systèmes informels de transfert de fonds pour effectuer diverses transactions manifestent également un réel intérêt pour la **rapidité** et l'efficacité de ces modes particuliers de transit financier.

La manière dont fonctionnent les systèmes informels de transfert de fonds est simple: le courtier livre l'argent à partir de sa réserve personnelle ou en utilisant son compte ouvert (les courtiers opèrent à compte courant) à la demande d'un autre courtier pour lequel un client est entré en contact. Dans le pays A, un client fournit une somme d'argent au courtier, en échange de quoi, le montant équivalent, converti en devises du pays du destinataire, est remise à une autre personne dans le pays B. Le système est efficace en raison d'un réseau complexe de relais pouvant s'appuyer sur la logistique des pays modernes où l'ordinateur règne en maître.

Comme le financement d'activités terroristes est susceptible de provenir souvent de sources illégales, les systèmes informels de transfert de fonds servent donc au transit de capitaux en provenance de trafics divers. la base des travaux d'un certain nombre de chercheurs, que dans certains cas, l'*hawala* servirait au blanchiment d'argent et à recycler des sommes d'argent issues de la contrebande de l'or

Dans cet ordre d'idées, fait état d'un rapport publié en 2002 par les spécialistes de l'ONU où il est confirmé que les enquêteurs privés aux trousses des capitaux d'al-Quaïda « se heurtent au système traditionnel de transfert de fonds, la hawala ». Ainsi, « des sommes de toutes importances se déplacent sur simple appel téléphonique avec échange de mots-codes convenus ».

2.3.9 Les terroristes utilisent également les systèmes bancaires officiels

Les conclusions auxquelles parvient le GAFI en matière de blanchiment d'argent et de financement d'activités terroristes sont cruciales. En effet, selon le GAFI les organisations criminelles et les groupes terroristes utilisent les mêmes circuits et les mêmes méthodes pour blanchir de l'argent, « déplacer des fonds ou dissimuler les liens avec leurs activités »

Pour le GAFI, distinguer entre les opérations à des fins de blanchiment de capitaux non liées au terrorisme et celles qui sont effectivement liées au terrorisme réside principalement dans le fait que

« l'un des individus impliqués dans le mécanisme figure sur une des listes publiées par le Conseil de sécurité des Nations Unies ». En fait, les informations actuelles ne permettent pas dans tous les cas de tracer une ligne claire entre ce qui relève de l'utilisation effective par des individus ou des groupes terroristes des systèmes informels de transfert de fonds. Ainsi, dans le cas des événements du 11 septembre, les opinions divergent quant à savoir si les participants ont eu recours aux systèmes informels de transfert de fonds.

Les autorités américaines ont pu établir le profil des différents pirates de l'air et de leur activité financière au cours de la période qui a précédé les attentats du 11 septembre. L'analyse effectuée par les États-Unis confirme que les opérations effectuées par les personnes concernées ont été relativement peu importantes et que, dans la plupart des cas, le système financier classique a été utilisé pour créer les comptes, transférer les fonds et régler les dépenses (GAFI, 2004).

Incidemment, le GAFI déploie ses énergies à retracer les mouvements de fonds qui seraient reliés au financement d'activités terroristes. De fait, en matière de transfert de fonds ou de virement, il importe de se référer, à l'instar du GAFI, à la définition suivante: « il s'agit de toute transaction financière opérée par une personne en se servant d'une institution financière et effectuée par des moyens électroniques, avec l'intention manifeste de mettre une somme d'argent à la disposition d'une autre personne dans une autre institution financière » (GAFI, 2004). Ce sont les usages des transferts de fonds à des fins terroristes qui préoccupent le GAFI. En effet:

Le GAFI envisage plusieurs exemples concernant l'utilisation des transferts de fonds par des groupes terroristes. Ainsi, des fonds terroristes obtenus dans un pays A sont transférés à une organisation terroriste dans un pays B; une organisation terroriste utilise les transferts de fonds pour déplacer de l'argent pour promouvoir ses activités hors des frontières de son port d'attache; les transferts de fonds sont utilisés à l'intérieur d'une campagne de levée de fonds à des fins d'activités terroristes. Pour tous ces cas, c'est le système bancaire officiel qui fournit la logistique nécessaire et non pas les systèmes informels de transfert de fonds, en dépit des avantages qu'ils sont susceptibles de représenter.

- Contexte mondial et systèmes informels de transfert de fonds

dans un texte portant sur les systèmes informels de transfert de fonds, déplore l'empressement des médias américains à désigner les financements *hawala* comme les complices coupables du terrorisme sans analyser « les propres turpitudes américaines en la matière ».

- Les systèmes informels de transfert de fonds: partenaires de l'économie légale

Pour le, « les opérations des systèmes ITCV peuvent parfois se raccorder aux systèmes bancaires formels (par exemple, en recourant aux comptes bancaires de l'opérateur d'un service ITCV) ». L'interdépendance entre systèmes bancaires officiels, légaux, conventionnels et systèmes informels de transfert de fonds est mise en évidence par l'analyse du GAFI. En effet, « selon un membre du GAFI, les systèmes ITCV ont de plus en plus recours au système bancaire classique, notamment lorsqu'il s'agit de traiter d'importants volumes d'espèces ».

Précise que dans l'opération initiale les voies bancaires classiques ne sont pas utilisées, c'est dans la suite des opérations, lorsque le*hawaladar* désire transformer les devises en dollars, qu'il a recours à une institution financière. À cette étape les banques new-yorkaises comme la Citibank, *la Wall Street Exchange/Banking* ou le *Multinet Trust Exchange* bénéficieraient des transactions des systèmes informels de transferts de fonds et seraient en mesure de retirer des profits de ces mouvements de capitaux se déployant en marge de leurs places financières. En fait, l'auteur s'étonne que ce n'est qu'au lendemain des événements du 11 septembre 2001 que le monde occidental a semblé découvrir l'existence des systèmes informels de transfert de fonds. En effet:

Le recours aux systèmes informels de transfert de fonds est pourtant bien connu des services occidentaux puisque la CIA elle même s'en servait pour financer les moudjahidines afghans lors de la guerre contre l'Union Soviétique.

2.4 Blanchiment d'argent et financement du terrorisme : conjonctures nationales

Plus insidieux, parce qu'à un niveau international affirmé cette fois, nous pouvons remarquer l'insistance des textes légaux à associer ensemble deux réalités dont les caractéristiques intrinsèques et empiriques démontrent pourtant que les différences sont plus importantes que les similarités

Le blanchiment d'argent en lien avec le financement d'activités terroristes et le blanchiment d'argent en lien avec les organisations criminelles. Que la question du blanchiment d'argent dans le cas des

groupes terroristes soit systématiquement associée aux dimensions de ce problème sur la base des éléments connus obtenus à la suite des opérations de blanchiment d'argent orchestrées par les organisations criminelles ne peut nous surprendre. Après tout, le phénomène crime est rapidement accolé à tout ce qui est encadré par la loi. Les groupes terroristes et les organisations criminelles menacent les marchés économiques des sociétés démocratiques. Les réseaux parallèles de fonds sont utilisés pour effectuer des mouvements financiers. Les groupes terroristes et les organisations criminelles ont besoin d'argent pour rester en affaires. La liste des points communs toutefois ne peut constituer un prétexte suffisant pour ne pas tenter de dépasser la lecture qui est généralement soumis aux gouvernements, aux politiciens, aux organes de détection.

En effet, lorsque l'on prend en compte les aspects particuliers et les différences relatifs à la question du blanchiment d'argent pour le financement d'activités terroristes, il n'apparaît pas possible de recourir aux critères de référence qui prévalent en matière de blanchiment d'argent dans le cas des organisations criminelles.

Les autorités compétentes associent volontiers le blanchiment d'argent et le financement du terrorisme, en dépit des différences qui caractérisent ces deux activités.
Et considère que le financement du terrorisme consiste à réunir des capitaux pour la réalisation d'activités terroristes, très souvent « financement du terrorisme » et mouvements de capitaux ou blanchiment d'argent sont confondus dans les écrits des chercheurs, des légistes, des analystes gouvernementaux et des agences de régulation. Cela dit, plusieurs des méthodes utilisées par des groupes criminels pour blanchir de l'argent sont les mêmes que celles auxquelles les terroristes ont recours pour masquer la finalité des fonds (obtenus légalement ou non) dont ils disposent et pour ne pas révéler aux organes de contrôle les destinataires de ces mouvements financiers

2.4.1 L'obligation de divulguer les opérations douteuses : un sujet de controverse parmi les acteurs

Les institutions financières doivent identifier leurs clients et conserver des dossiers à cet effet.

En doit obliger les individus et les institutions de divulguer aux autorités compétentes l'existence de biens dont ils auraient été le propriétaire ou le dépositaire, biens qui serait liés, à leur connaissance, à des activités terroristes. En ce qui concerne les produits de la criminalité (blanchiment d'argent), il faut imposer aux institutions l'obligation de divulguer la possession de biens terroristes, à savoir l'obligation requise par la loi de déclarer « l'importation ou l'exportation d'espèces ou d'effets dans

certaines circonstances » est un lourd tribut pour la personne chargée de la transaction. Cette mesure ajoute un niveau de responsabilité injustifié à la personne responsable du moyen de transport vis-à-vis de ce que les passagers amènent dans leurs bagages

Considère aussi que les dispositions légales qui imposent aux individus et aux institutions de déterminer et de divulguer s'ils sont en possession ou s'ils contrôlent une propriété appartenant à un groupe terroriste posent des problèmes au niveau de la mise en œuvre.

Pour apprécier les conditions dans lesquelles les banques vont se soumettre aux exigences de la loi, il importe de ne pas sous-estimer la complexité du financement du terrorisme ainsi que les aspects spécifiques qui en caractérisent la dynamique, au risque, en effet, que les efforts déployés pour repérer et identifier l'origine et la finalité des sommes d'argent qui circulent via les centres financiers internationaux soient réduits à néant, précisément quand des questions se posent relativement à la légalité des transferts.

Au niveau mondial, en vertu des différentes lois qui s'appliquent, les banques sont tenues de procéder à certaines vérifications en ce qui a trait à leurs clients et en ce qui concerne des sommes d'argent importantes déposées dans leurs succursales. Il y aurait peut-être lieu de noter, à la suite du GAFI (Directives à l'attention des institutions financières pour la détection des activités de financement du terrorisme, 24 avril 2002), que les institutions financières sont incapables de détecter en soi le financement du terrorisme. Le seul indice vraiment révélateur serait qu'un terroriste ou une organisation connus ouvrirait un compte. En effet, les difficultés auxquelles les banques sont confrontées sur une base quotidienne constituent des obstacles à l'identification des clients, en raison de l'impossibilité, dans certains cas, d'obtenir les informations nécessaires pour garantir l'exactitude des données susceptibles de permettre de repérer le financement du terrorisme:

2.4.2 Blanchiment d'argent et dynamiques spécifiques des groupes terroristes

Certains cas d'étroite relation entre des groupes terroristes et des organisations criminelles a favorisé une interprétation de tout ce qui touche au blanchiment d'argent comme étant de même nature pour ces deux groupes. Dans le cadre de la discussion actuelle, pour un examen du blanchiment d'argent qui insiste sur les différences entre ce qui passe pour les groupes terroristes et ce qui se passe pour les organisations criminelles. Ainsi, nous serons en mesure de mettre en évidence que le

financement d'activités terroristes et le blanchiment d'argent ne se recoupent pas nécessairement en toutes circonstances et que pour traduire la pluralité des activités de financement du terrorisme, se référer à ce qui se passe pour les organisations criminelles ne suffit pas.

2.4.3 Distinguer entre « blanchiment d'argent » (un délit passé) et « financement du terrorisme » (une activité future)

Sur la base des écrits des chercheurs et des analystes, un constat s'impose : se référer à ce qui passe pour les organisations criminelles ne peut traduire la complexité du terrorisme. Plusieurs éléments d'importance devraient donc être pris en considération lorsque l'on tente de comprendre de quelle manière les groupes terroristes procèdent au blanchiment d'argent en vue de financer des activités terroristes. Par exemple, le terrorisme n'a pas nécessairement besoin de sommes astronomiques pour se réaliser; selon le département d'État des États-Unis, « les sommes que les cellules terroristes ou leurs membres cherchent à occulter » sont parfois minimes lorsqu'elles sont comparées « aux sommes recyclées par la criminalité organisée et par les grands trafiquants de stupéfiants ». En fait, les lois qui ont été adoptées visaient, au départ, la lutte contre le blanchiment des capitaux. C'est ainsi que le département d'État constate l'inutilité et l'inefficacité de la nécessité de déclarer les dépôts de plus de 10 000 $ dans le cas du financement d'activités terroristes.

Diverses opérations financières au moyen d'instruments financiers multiples sont utilisées de manière à permettre que l'argent blanchi soit investi à nouveau, soit dans des activités légales, soit pour financer des trafics divers, ou encore pour servir à des activités terroristes. Les mêmes auteurs définissent le financement du terrorisme comme **le traitement de biens d'une source quelconque (légale ou non) aux fins du financement d'une activité terroriste passée ou future**. En fait, voilà bien une caractéristique qui permet de distinguer entres elles les opérations de blanchiment d'argent et les activités de financement du terrorisme : plus souvent qu'autrement, le financement du terrorisme est orienté vers des activités futures. Pourtant, aux termes de la loi antiterroristes donc,

Il est possible que la seule infraction commise au moment du financement soit une conspiration en vue d'un acte terroriste ».

Rappelons que de nombreux observateurs dans les médias, de même que des chercheurs dans leurs écrits, ont déjà mis en exergue que le terrorisme est différent du blanchiment d'argent, on établit une distinction majeure entre le blanchiment d'argent (résultant de crimes commis par des groupes ou des associations criminelles) et le financement du terrorisme pouvant emprunter des voies légitimes ou illégales .

Suite au blanchiment d'argent, d'importantes sommes d'argent sont réinjectées dans l'économie légale d'un pays pour être utilisables à des fins multiples et variées sans que l'origine des fonds soit connue des autorités compétentes. À l'évidence, ceci implique nécessairement la commission préalable de crimes qui aient produits les fonds à blanchir. Incidemment, il est intéressant de noter que le département d'État des États-Unis parvient aux mêmes conclusions.

Le financement du terrorisme est différent du blanchiment des capitaux à de nombreux égards. D'habitude, les blanchisseurs d'argent recyclent les fonds issus d'activités criminelles pour qu'ils puissent être utilisés à des fins légitimes ou criminelles. Les fonds qui servent à financer l'activité terroriste sont obtenus principalement au moyen de la collecte de dons effectuée souvent par des organismes licites sans but lucratif, bien que les groupes terroristes aient aussi recours à des activités criminelles pour se procurer des fonds.

Ainsi, le département d'État met en évidence l'ambiguïté soulevée par l'intention manifeste des lois d'associer ensemble, en dépit de leurs différences, le blanchiment d'argent résultant d'un crime et le financement de l'activité criminelle qu'est le terrorisme. En effet, les fonds « qui servent à financer le terrorisme ne proviennent pas d'habitude d'un crime ou d'un délit antérieur » Le caractère criminel des fonds ne se confirme que dans l'intention des groupes terroristes :

Soit ils tentent de faciliter l'exécution d'un acte terroriste.

Soit ils essaient de financer une organisation terroriste particulière à l'étranger.

En définitive, en ce qui touche le financement du terrorisme, il peut provenir d'activités légales, comme les collectes de fonds auprès de communautés ciblées ou encore les opérations commerciales menées par des entreprises légales diverses, dont les dirigeants ont des liens de proximité variable avec des groupes terroristes. Évidemment, les fonds peuvent également provenir d'activités illégales diverses comme le trafic de stupéfiants, la contrebande d'armes et d'autres produits, la fraude, des enlèvements ou l'extorsion. Dans ces cas il importe alors pour les terroristes de procéder à des transactions économiques de blanchiment d'argent, tout comme n'importe quelles organisations criminelles.

Quant aux activités légitimes qui servent au financement d'opérations terroristes, le cas de la cueillette de fonds auprès de certaines communautés culturelles, prétextant souvent une cause charitable est particulière. Il est question d'une catégorie hybride, ici, relevant à la fois d'un contexte

légitime (les œuvres de charité) et d'une situation pouvant être qualifiée de frauduleuse. En effet, sous couvert d'activités reliées à des œuvres de bienfaisance, des sommes d'argent sont détournées de leur finalité annoncée. Dans certains cas les partisans d'organisations terroristes qui occupent des postes clés dans des organismes charitables peuvent détourner des fonds pour des causes terroristes à l'insu des donateurs.

2.4.4 Utilisation du réseau bancaire officiel et des systèmes de transfert de fonds : les groupes terroristes ont accès à des sources légitimes de revenus

Les contributions des chercheurs ainsi que les rapports gouvernementaux mettent en évidence l'importance du lien entre les sources de financement d'activités terroristes et les moyens par lesquels les fonds sont transférés à leurs destinataires. Il importe donc de s'intéresser aux moyens utilisés par les organisations criminelles et par les groupes terroristes pour faire transiter des fonds destinés à leurs opérations respectives. De nombreuses voies sont disponibles pour procéder au transfert de fonds, que ces sommes d'argent proviennent d'activités criminelles ou d'activités légales, en lien, par exemple avec des sociétés commerciales qui opèrent en toute légitimité (des agences de voyage ou des entreprises d'import-export qui sont, toutefois, la plupart du temps des sociétés écrans). Les fonds destinés à des fins terroristes sont susceptibles d'emprunter des circuits multiples, autant par les réseaux bancaires officiels que par les réseaux financiers parallèles (*hawalas*). En outre, dans certains cas de l'argent comptant, de l'or ou d'autres valeurs sont tout simplement transportés physiquement. En général, l'utilisation de voies multiples de transferts de fonds, dont le système bancaire officiel, sert à masquer la destination finale des fonds. Ainsi, les terroristes envoient le fruit des activités de financement vers des pays comprenant des centres financiers majeurs.

Certains pays ne sont pas disposés à se conformer aux directives et aux normes internationales en matière de déclaration de transferts de fonds d'origine suspecte. Par exemple, des terroristes, dont les activités se déploient au niveau international ont recours à des banques pour une grande partie de leurs transactions et de leurs mouvements bancaires. Or, ces dernières ne se sentiraient pas tenues, au même titre que les banques et les établissements financiers occidentaux ayant pignon sur rue dans des pays signataires de la Résolution 1373 des Nations Unies, de signaler tous les cas de transferts de fonds douteux.

En fin de compte, le blanchiment d'argent concerne des sommes importantes d'argent qui transitent « rapidement dans des réseaux financiers locaux et internationaux », tandis qu'en ce qui a trait au financement d'activités terroristes, il est question « de plus petites sommes d'argent qui passent par des centres financiers internationaux ».

Le blanchiment d'argent et le financement des activités terroristes sont presque toujours des opérations transnationales.

2.4.5 Les procédés de blanchiment d'argent des groupes terroristes recoupent en partie ceux des organisations criminelles

Les modes de blanchiment d'argent utilisés par les associations criminelles et les groupes terroristes sont techniquement en grande partie les mêmes. Toutefois, en l'absence de preuves ou d'éléments suffisants pour appuyer les conjectures des organes de surveillance, les modalités de blanchiment d'argent qui ont la faveur des terroristes restent des suppositions jusqu'à preuve du contraire. Sur la base d'informations contenues dans le guide à l'Intention des comptables agréés et les divers documents produits par le GAFI, nous recensons certaines des techniques pouvant être utilisées dans le blanchiment d'argent en lien avec le financement d'activités terroristes.

- Utiliser des prête-noms ou des mandataires :

Il s'agit de l'utilisation de membres de la famille, de proches qui sont reconnus dans la communauté et qui pourront faire des transactions pour le compte des terroristes. Comme les terroristes assument de plus en plus que pour cibler les opérations financières douteuses, les institutions financières et les organes de surveillance utilisent les listes de terroristes et d'organismes de charité considérés par la *Loi antiterroriste* comme ayant des liens avec des groupes terroristes, les individus et les groupes terroristes ont recours à des amis ou à des associés des membres de la famille pour procéder aux opérations bancaires et espérer ainsi éviter d'éveiller les soupçons. Des structures sociétaires ou des fiducies peuvent également servir de prête-noms. Il s'agit de compliquer et d'obscurcir les chemins empruntés par l'argent.

- Le « schtroumpfage » :

Soit les dépôts ou des retraits fractionnés sur des comptes bancaires. Des opérations de valeur inférieure aux montants susceptibles d'attirer l'attention des organes de contrôle et d'être qualifiées d'opérations douteuses sont effectuées par des personnes tout à fait ordinaires.

- Achat au comptant de biens de grande valeur :

Des objets de grande valeur sont payés en argent comptant et sont enregistrés sous le nom d'amis bienveillants par les individus ou les groupes qui cherchent à blanchir de l'argent.

- Le recours aux bureaux de change :

Les blanchisseurs achètent des devises étrangères en grande quantité qui peuvent être ensuite transférées dans des comptes ouverts dans diverses banques à travers le monde.

- La contrebande de devises :

Soit ses mouvements de fonds clandestins en espèces (par des passeurs ou des envois d'argent en vrac). Les blanchisseurs font transiter des grosses sommes d'argent par courrier, par services de messagerie ou par des individus qui transportent sur eux l'argent à destination de pays qui sont favorables au secret bancaire: l'origine et la propriété des fonds ne sont pas susceptibles d'être divulguées.

- Les jeux de hasard au casino *:*

En échangeant de l'argent contre des jetons, l'argent qui n'a pas été utilisé est récupéré sous forme de chèque.

- Les achats de diverses catégories d'instruments monétaires :

Chèques de voyage, chèques bancaires, mandats.

- L'utilisation de cartes de crédit ou de débit et les virements

- Les secteurs vulnérables de l'économie

« Les lois en vigueur relatives au blanchiment des capitaux d'une façon tout à fait différente » et de se tourner vers d'autres mesures plus adaptées aux mouvements de fonds des terroristes. En outre, les groupes terroristes utilisent souvent des fonds provenant de sources légales pour financer leurs opérations terroristes.

Le blanchiment d'argent est **la transformation du produit d'une infraction sous une forme utile*:***

Le secteur des valeurs mobilières comme étant particulièrement vulnérable au regard du blanchiment de capitaux. En outre, il y a des risques potentiels que les marchés des métaux et des pierres précieuses, surtout le commerce de l'or et du diamant, soient très prisés par les groupes terroristes pour procéder au blanchiment de capitaux. La confusion de produits légaux et illégaux dans les comptes de sociétés de négoces de diamants et, en général, dans les entreprises ayant des liens avec les groupes terroristes, complique l'identification des procédés couramment utilisés pour blanchir de l'argent. On ne peut parler dans biens des cas que d'indices de liens avec le financement du terrorisme.

CONCLUSION

Les Nations Unies (ONU) ont consenti de nombreux efforts, en grande partie sous forme de traités internationaux, pour lutter contre le terrorisme et les mécanismes utilisés pour le financer.

Même avant l'attaque du 11 septembre aux États-Unis, l'ONU disposait de la Convention internationale pour la répression du financement du terrorisme (1999) qui stipule que :

-Commet une infraction au sens de la présente Convention toute personne qui, par quel que moyen que ce soit, directement ou indirectement, illicitement et délibérément, fournit et réunit des fonds dans l'intention de les voir utiliser ou en sachant qu'ils seront utilisés, en tout ou partie, en vue de commettre, Un acte qui constitue une infraction au regard et selon la définition de l'un des traités énumérés en annexe ; ou tout autre acte destiné à tuer ou blesser grièvement un civil, ou toute autre personne qui ne participe pas directement aux hostilités dans une situation de conflit armé, lorsque, par sa nature ou son contexte, cet acte vise à intimider une population ou à contraindre un gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque.

Guide de référence sur la lutte contre le blanchiment de capitaux et contre le financement du terrorisme, le problème pour certains pays est de définir le terrorisme.

Tous les pays qui ont adopté la convention ne sont pas d'accord sur les actes qu'il faut considérer comme 'terroristes'. La signification du terrorisme n'est pas acceptée universellement du fait des importantes implications politiques, religieuses et nationales qui diffèrent d'un pays à l'autre.

Le GAFI, qui est également reconnu comme l'organisme international d'établissement de normes en matière de lutte contre le financement du terrorisme (LFT), ne définit pas spécifiquement le terme 'financement du terrorisme' dans ses huit Recommandations Spéciales sur le financement du terrorisme *(Recommandations Spéciales)* élaborées après les événements du 11 septembre 2001. Toutefois, le GAFI recommande aux pays de ratifier et

de mettre en œuvre la Convention internationale des Nations unies pour la répression du financement du terrorisme, ainsi la définition précitée est celle qu'ont adoptée le plus de pays en matière de financement du terrorisme.

Je suis contre la violence, non seulement parce que je la crois immorale, mais aussi parce que je la vois inefficace. Il ne peut y avoir de changements durables positifs de la société que ceux qui permettent la possession tranquille d'un acquis. Or, il n'y a pas de possession tranquille de ce qui a

été obtenu pas la force aussi longtemps qu'un large consensus ne s'est pas établi quant à la légitimité de cette possession, ce qui est d'autant plus long qu'a été brutale la force employée.

Guerres et révolutions sanglantes peuvent être évitées car ce sont désormais des alliances et non des individus qui ont le pouvoir et les liens qui assurent la cohésion d'une alliance peuvent être détruits par les armes de la persuasion au profit d'une alliance rivale. La violence est une solution de facilité. Une solution d'impatience, sans intelligence, qui modifie les effets sans changer les causes et dont les résultats bénéfiques ne peuvent donc être permanents, alors que les dommages causés sont bien lents à réparer.

<u>Pour la paix</u>
Il y a un temps pour tout,
et chaque chose a son heure sous le ciel.
Il est (…) un temps pour tuer et un temps pour guerir,
un temps pour demolir et un temps pour batir ;
(…) un temps pour jeter des pierres et un temps pour ramasser des pierres ;
un temps pour embrasser et un temps pour repousser les caresses ;
(…) un temps pour aimer et un temps pour hair,
un temps pour la guerre et un temps pour la paix.
(l'Ecclesiaste)

Annexe A

Historique (CYBER- TERRORISTE)

1- L'historique du cyber-terrorisme montre que les attaques évoquées précédemment ne sont pas seulement théoriques. Sans être exhaustif, voici quelques événements marquants dans
L'histoire du cyber-terrorisme :

- En 1996, un sympathisant du mouvement américain White Supremacist a attaqué et temporairement mis hors service un ISP qui tentait de l'empêcher d'envoyer en masse des messages racistes. L'attaquant avait alors envoyé le message prémonitoire suivant : "Vous n'avez pas encore vu de vrai terrorisme électronique. C'est une promesse".

- En 1997 et les années suivantes, des sympatisants du mouvement Zapatiste mexicain ont effectué des intrusions à plusieurs reprises dans les systèmes logistiques mexicains et ont contribué à influencer l'opinion publique en faveur des Zapatistes, dont la situation, face à l'armée mexicaine, était critique. Des agents d'influence ont propagé des rumeurs sur l'instabilité du Peso mexicain, ce qui a
conduit à un effondrement de celui-ci, obligeant le gouvernement à négocier avec les rebelles.

- En 1998, des militants espagnols ont attaqué l'IGC américain (Institute for Global Communications) en effectuant un mail bombing en direction des responsables de l'ISP et des commandes effectuées avec de faux numéros de carte bancaire. Ils menaçaient en outre d'attaquer les autres clients de l'ISP. Ces militants reprochaient à l'IGC d'héberger le site Web du journal Euskal Herria, une publication basée à New York et soutenant le mouvement indépendantiste Basque, et en particulier de soutenir le terrorisme car une partie du site contenait des informations concernant l'ETA. L'IGC a fini par retirer le site incriminé.

- En 1998, la guerrila Tamoule dans le nord du Ski Lanka a engorgé les serveurs des ambassades ski-lankaises avec environ 800 e-mails par jour pendant deux semaines. Les e-mails contenaient le message suivant: "Nous sommes les Tigres Noirs d'Internet et nous allons interrompre vos communications". Les services de renseignement ont qualifié ces attaques comme étant les premières attaques connues de terroristes contre les systèmes informatiques d'un état.

2- D'autres exemples non datés sont plus difficilement vérifiables: en Floride, des attaquants auraient détourné les appels au 911 (la police, aux Etats-Unis) vers un magasin de pizzas à emporter. Plus grave, au Massachusetts, un pirate a provoqué la coupure des communications d'une tour de contrôle de la FAA pendant 6 heures. En Russie, des pirates auraient utilisé un collaborateur interne de Gazprom (organisme qui détient le monopole du pétrole en Russie) pour implanter un cheval de Troie leur permettant d'obtenir le contrôle du système de distribution qui gère les flux de pétrole dans les pipe-lines.

- En 1999, pendant le conflit du Kosovo, les ordinateurs de l'OTAN ont été les cibles de mail bombing et de tentatives de dénis de service de la part d'opposants aux bombardements de l'OTAN, dont certains situés dans les états en conflit. Les serveurs de l'OTAN ont été plusieurs fois mis hors service pendant plusieurs jours.

- En 1999, après le bombardement "non tactique" de l'ambassade chinoise à Belgrade,des attaquants chinois ont déposé des messages du type "nous ne cesserons d'attaquer jusqu'à ce que la guerre s'arrête" sur des sites gouvernementaux américains.

- En février 2001, un serveur (heureusement de développement) du fournisseur d'électricité California ISO a été laissé connecté à Internet pendant 11 jours et, bien sûr, hacké.

- En avril 2001, après la collision au dessus de la Chine entre un avion espion américain et un chasseur chinois, et l'incarcération de l'équipage américain en Chine, des groupes de hackers des deux camps (comme les groupes "Honker Union of China" et "Chinese Red Guest Network Security Technology Alliance", en Chine) se sont menés une guerre violente. Plus de 1200 sites américains ont été défigurés ou cibles

d'attaques de type déni de service distribué (DDoS), dont les sites de la Maison Blanche, de l'US Air Force, du Département de l'Energie, mais aussi d'entreprises diverses.

- En août 2001, le ver Code Red, qui s'est propagé à très grande vitesse sur Internet, faisait apparaître le message "Hacked by Chinese". Même si aucune preuve n'atteste avec certitude que ce ver provient de Chine, on ne peut s'empêcher de mettre ce message en relation avec les attaques de 1999 (cf ci-dessus). La charge utile de ce ver consistait à établir un grand nombre de connexions vers le site Web de la Maison Blanche afin de provoquer un déni de service distribué. Depuis, d'autres vers (Nimda, Slammer par exemple) ont défrayé la chronique.

- Si l'on considère que la défiguration de sites Web constitue le tout premier degré de cyber-attentat, on peut étudier les conflits Inde/Pakistan et Israël/Palestine depuis 1999 jusqu'à aujourd'hui à l'aune des défigurations de sites appartenant aux différentes parties. On observe un strict parallèle entre le nombre de défigurations de sites et les événements politiques et militaires dans les régions citées. Cette comparaison révèle une connexion intime entre les conflits qui ont lieu dans le monde physique et dans le monde virtuel.

- En 2001 et 2002, plusieurs documents retrouvés en Afghanistan et lors des enquêtes sur les réseaux d'Al Qaida ont montré que le cyber-terrorisme était activement étudié par Oussama Ben Laden, passionné par ce type de guerre moderne. Il a consacré des sommes importantes au recrutement dans le monde arabe des meilleurs informaticiens et spécialistes d'Internet. Un plan en ce sens lui avait été remis en juin 2001 par un intégriste séoudien de Londres. D'ailleurs, depuis la capitale britannique, les réseaux Internet intégristes sont de plus en plus actifs.

Annexe B

PROJETS DE GAFI (QUARANTE RECOMMANDATIONS)

Introduction

Les méthodes et techniques de blanchiment de capitaux évoluent au gré des contre-mesures qui sont déployées. Ces dernières années, le Groupe d'action financière (GAFI) a pris note du développement de combinaisons sophistiquées de techniques, telles que l'usage croissant de **personnes morales** afin de dissimuler la véritable propriété et le véritable contrôle des produits d'activités illicites, ainsi que le recours accru à des professionnels pour obtenir des conseils et de l'assistance afin de blanchir des fonds criminels. Ces facteurs, associés à l'expérience acquise par le GAFI dans le cadre du processus des Pays et Territoires Non Coopératifs et à de nombreuses initiatives nationales et internationales, ont incité le GAFI à réexaminer et réviser les Quarante Recommandations, et à créer un nouveau cadre complet de lutte contre le blanchiment de capitaux et le financement du terrorisme. Le GAFI invite désormais tous les pays à prendre les mesures nécessaires de mise en conformité de leurs systèmes nationaux de lutte contre le blanchiment de capitaux et le financement du terrorisme avec les nouvelles Quarante Recommandations, et à mettre efficacement ces mesures en œuvre

.

Le processus de révision des Quarante Recommandations a été approfondi, ouvert aux membres du GAFI, aux non-membres, aux observateurs, au secteur financier et autres secteurs concernés et à toute autre partie intéressée. Cette consultation a généré un large éventail de contributions dont il a été tenu compte dans le processus de révision

.

Les Quarante Recommandations révisées s'appliquent désormais non seulement au blanchiment de capitaux mais aussi au financement du terrorisme, et, combinées avec les Huit Recommandations Spéciales sur le financement du terrorisme, elles créent un cadre de mesures renforcé, étendu et cohérent pour lutter contre le blanchiment de capitaux et le financement du terrorisme. Le GAFI reconnaît que les pays sont dotés de systèmes juridiques et financiers divers, et qu'en conséquence, tous ne peuvent pas prendre de mesures identiques afin de réaliser l'objectif commun, notamment lorsqu'il s'agit de mesures détaillées d'application. Les Recommandations établissent des normes minimales qui requièrent l'adoption par les pays de mesures de mise en œuvre précises, et ce en fonction de leurs circonstances particulières et de leurs cadres constitutionnels. Les Recommandations recouvrent l'ensemble des mesures que chaque système national devrait appliquer en matière de justice pénale et de systèmes de contrôle, les mesures préventives qui doivent être adoptées par les institutions financières et autres entreprises ou professions, ainsi que la coopération internationale.

Les premières Quarante Recommandations ont été formulées en 1990 dans l'optique de lutter contre l'usage abusif des systèmes financiers à des fins de blanchiment de l'argent de la drogue. Les Recommandations ont été révisées une première fois en 1996 afin de refléter l'évolution des typologies de blanchiment de capitaux. Les Quarante Recommandations telles que révisées en 1996 ont été adoptées par plus de 130 pays et constituent la norme internationale en matière de lutte contre le blanchiment de capitaux.

En octobre 2001, le GAFI a étendu son mandat à la question du financement du terrorisme et a franchi un pas important en adoptant les Huit Recommandations Spéciales sur le financement du terrorisme. Ces Recommandations contiennent une série de mesures visant à combattre le financement des actes et des organisations terroristes et complètent les Quarante Recommandations.

La nécessité de surveiller et d'évaluer les systèmes nationaux au regard de ces normes internationales est un élément clé dans la lutte contre le blanchiment de capitaux et le financement du terrorisme. Les évaluations mutuelles conduites par le GAFI et les organismes régionaux de type GAFI, ainsi que les évaluations menées par le FMI et la Banque Mondiale constituent un mécanisme vital permettant de s'assurer de la mise en œuvre effective des Recommandations du GAFI par tous les pays et territoires.

[1] Le GAFI est un organisme intergouvernemental qui établit des normes, développe et assure la promotion de politiques de lutte contre le blanchiment de capitaux et le financement du terrorisme. Il se compose actuellement de 33 membres : 31 pays et gouvernements et de deux organisations internationales ; de plus de 20 observateurs : 5 organismes régionaux de type GAFI et plus de 15 autres organisations ou organismes internationaux. La liste des membres et observateurs peut être consultée sur ce site.

[2] Les Quarante Recommandations et les Huit Recommandations Spéciales du GAFI ont été reconnues par **le Fonds Monétaire International** et **la Banque Mondiale** comme les normes internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

SYSTEMES JURIDIQUES

Champ d'application de l'infraction de blanchiment de capitaux

Recommandation 1

Les pays devraient incriminer le blanchiment de capitaux sur la base de **la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes, 1988 (Convention de Vienne)** et de **la Convention des Nations Unies contre la criminalité transnationale organisée, 2000 (la Convention de Palerme)**.

Les pays devraient appliquer l'infraction de blanchiment de capitaux à toutes les infractions graves, afin de couvrir la gamme la plus large possible d'infractions sous-jacentes. Les infractions sous jacentes peuvent être définies par rapport à l'ensemble des infractions, ou par rapport à un seuil lié soit à une catégorie d'infractions graves, soit à la peine privative de liberté dont est passible l'infraction sous-jacente (méthode du seuil), ou par rapport à une liste d'infractions sous-jacentes ou par rapport à une combinaison de ces méthodes.

Dans les pays qui adoptent la méthode du seuil, les infractions sous-jacentes devraient au minimum comprendre toutes les infractions relevant de la catégorie des infractions graves en vertu de leur droit interne, ou devraient inclure les infractions qui sont passibles d'une peine maximale de plus d'un an d'emprisonnement ou, pour les pays qui ont un seuil minimum pour les infractions dans leur système juridique, les infractions sous-jacentes devraient englober toutes les infractions passibles d'une peine minimale de plus de six mois d'emprisonnement.

Quelle que soit l'approche adoptée, chaque pays devrait au minimum inclure une gamme d'infractions au sein de chacune des catégories désignées d'infractions.

Les infractions sous-jacentes du blanchiment de capitaux devraient couvrir les actes commis dans un autre pays, qui constituent une infraction dans ce pays, et qui auraient constitué une infraction sous-jacente s'ils avaient été commis sur le territoire national. Les pays peuvent prévoir que la seule condition requise est que les actes auraient été qualifiés d'infractions sous-jacentes s'ils avaient été commis sur le territoire national.

Les pays peuvent déterminer que l'infraction de blanchiment de capitaux ne s'applique pas aux personnes qui ont commis l'infraction sous-jacente, lorsque les principes fondamentaux de leur droit interne l'exigent.

Recommandation 2

Les pays devraient s'assurer que :

a) L'élément intentionnel et la connaissance des faits requis pour établir la preuve de l'infraction de blanchiment de capitaux sont conformes aux normes précisées dans les Conventions de Vienne et de Palerme, étant entendu que l'élément intentionnel pourrait être déduit de circonstances factuelles objectives.

b) La responsabilité pénale, et si ce n'est pas possible, la responsabilité civile ou administrative devrait s'appliquer aux personnes morales. Ceci n'exclut pas, le cas échéant, les poursuites parallèles, qu'elles soient pénales, civiles ou administratives à l'encontre de personnes morales dans les pays où ce type de responsabilité est prévu par la loi. Les personnes morales devraient pouvoir faire l'objet de sanctions efficaces, proportionnées et dissuasives. Ces mesures ne devraient pas porter atteinte à la responsabilité pénale des personnes physiques.

Mesures provisoires et confiscation

Recommandation 3

Les pays devraient adopter des mesures similaires à celles indiquées dans les Conventions de Vienne et de Palerme, y compris des mesures législatives, afin que leurs autorités compétentes soient en mesure de confisquer les biens blanchis, les produits découlant du blanchiment de capitaux ou des infractions sous-jacentes, ainsi que les instruments utilisés ou destinés à être utilisés pour

commettre ces infractions, ou des biens d'une valeur équivalente, sans préjudice du droit des tiers de bonne foi.

De telles mesures devraient permettre (a) d'identifier, retrouver et estimer les biens faisant l'objet d'une mesure de confiscation ; (b) de mettre en œuvre des mesures provisoires, telles le gel et la saisie, afin de faire obstacle à toute transaction, transfert ou cession de ces biens; (c) de prendre des mesures pour empêcher ou annuler des actes visant à priver l'État de sa faculté à recouvrer des biens faisant l'objet d'une mesure de confiscation ; et (d) de prendre toutes les mesures d'enquête appropriées.

Les pays peuvent envisager d'adopter des mesures permettant la confiscation de tels produits ou instruments sans condamnation pénale préalable, ou des mesures faisant obligation à l'auteur présumé de l'infraction d'établir la preuve de l'origine licite des biens présumés passibles de confiscation, dans la mesure où une telle obligation est conforme aux principes de leur droit interne.

MESURES À PRENDRE PAR LES INSTITUTIONS FINANCIERES ET LES ENTREPRISES ET PROFESSIONS NON FINANCIERES POUR LUTTER CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

Recommandation 4

Les pays devraient veiller à ce que les lois sur le secret professionnel des institutions financières n'entravent pas la mise en œuvre des Recommandations du GAFI.

Devoir de vigilance (« due diligence ») relatif à la clientèle et devoir de conservation des documents

Recommandation 5

Les institutions financières ne devraient pas tenir de comptes anonymes, ni de comptes sous des noms manifestement fictifs.

Les institutions financières devraient prendre les mesures de vigilance (« due diligence ») à l'égard de la clientèle, notamment en identifiant et en vérifiant l'identité de leurs clients, lorsque :

- elles nouent des relations d'affaires ;
- elles effectuent des transactions occasionnelles : (i) supérieures au seuil désigné applicable ; ou (ii) sous forme de virements électroniques dans les circonstances visées par la Note interprétative de la Recommandation Spéciale VII ;
- il y a suspicion de blanchiment de capitaux ou de financement du terrorisme ;

- ou l'institution financière a des doutes quant à la véracité ou à la pertinence des données d'identification du client précédemment obtenues.

Les mesures de vigilance à l'égard de la clientèle sont les suivantes :

a) Identifier le client et vérifier son identité au moyen de documents, données et informations de source fiable et indépendante.

b) Identifier le bénéficiaire effectif, et prendre des mesures raisonnables pour vérifier cette identité de telle manière que l'institution financière ait une connaissance satisfaisante de l'identité du bénéficiaire effectif. Ceci inclut pour les personnes morales et les constructions juridiques, que les institutions financières prennent également des mesures raisonnables pour comprendre la propriété et la structure de contrôle du client.

c) Obtenir des informations sur l'objet et la nature envisagée de la relation d'affaires.

d) Exercer une vigilance constante à l'égard de la relation d'affaires et assurer un examen attentif des transactions effectuées pendant toute la durée de cette relation d'affaires, afin de s'assurer que les transactions effectuées sont cohérentes avec la connaissance qu'a l'institution de son client, de ses activités commerciales, de son profil de risque et, lorsque cela est nécessaire, de l'origine des fonds.

Les institutions financières devraient mettre en œuvre chacune des mesures de vigilance figurant aux paragraphes (a) à (d) ci-dessus, mais elles peuvent déterminer l'étendue de ces mesures en fonction du niveau de risque associé au type de clientèle, de relation d'affaires ou de transaction. Les mesures prises devraient être conformes aux lignes directrices mises en place par les autorités compétentes.

Pour les catégories à plus haut risque, les institutions financières devraient prendre des mesures de vigilance renforcée. Dans des circonstances déterminées, lorsque les risques sont faibles, les pays peuvent décider d'autoriser les institutions financières à appliquer des mesures réduites ou simplifiées.

Les institutions financières devraient vérifier l'identité du client et du bénéficiaire effectif avant ou au moment de l'établissement d'une relation d'affaires, ou lorsqu'elles effectuent des transactions pour des clients occasionnels. Les pays peuvent autoriser les institutions financières à achever ces vérifications, dans des délais aussi brefs que possible, après l'établissement de la relation, si les risques de blanchiment de capitaux sont gérés de façon efficace et s'il est essentiel de ne pas interrompre le déroulement normal de la relation d'affaires.

Si l'institution financière ne peut pas se conformer aux obligations découlant des paragraphes (a) à (c) ci-dessus, elle ne devrait pas ouvrir de compte, nouer de relation d'affaires ou effectuer une transaction ; ou devrait mettre un terme à la relation d'affaires ; et devrait envisager de faire une déclaration d'opérations suspectes concernant ce client.

Ces obligations devraient s'appliquer à tous les nouveaux clients, néanmoins les institutions financières devraient les appliquer également aux clients existants selon l'importance des risques qu'ils représentent et devraient mettre en œuvre des mesures de vigilance sur ces relations existantes aux moments opportuns.

(Voir les notes interprétatives pour la Recommandation **5** et les **Recommandations 5, 12 et 16**)

[4] Les documents, données et informations de source fiable et indépendante sont désignés ci-après sous le terme "données d'identification".

Recommandation 6

Les institutions financières devraient, s'agissant de personnes politiquement exposées, mettre en œuvre les mesures de vigilance normales, et en outre :

a) Disposer de systèmes de gestion des risques adéquats afin de déterminer si le client est une personne politiquement exposée.

b) Obtenir l'autorisation de la haute direction avant de nouer une relation d'affaires avec de tels clients.

c) Prendre toutes mesures raisonnables pour identifier l'origine du patrimoine et l'origine des fonds.

d) Assurer une surveillance renforcée et continue de la relation d'affaires.

Recommandation 7

Les institutions financières devraient, en ce qui concerne les relations de correspondant bancaire transfrontalier et autres relations similaires, mettre en œuvre les mesures de vigilance normales, et en outre :

a) Rassembler suffisamment d'informations sur l'institution cliente afin de bien comprendre la nature de ses activités et d'évaluer, sur la base d'informations publiquement disponibles, la réputation de l'institution et la qualité de la surveillance, y compris vérifier si l'institution concernée a fait l'objet d'une enquête ou d'une intervention de l'autorité de surveillance ayant trait au blanchiment de capitaux ou au financement du terrorisme.

b) Évaluer les contrôles mis en place par l'institution cliente sur le plan de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

c) Obtenir l'autorisation de la haute direction avant de nouer de nouvelles relations de correspondant bancaire.

d) Préciser par écrit les responsabilités respectives de chaque institution.

e) Pour ce qui concerne les comptes « de passage » (« payable-through accounts »), s'assurer que la banque cliente a vérifié l'identité et a mis en œuvre les mesures de vigilance constante vis-à-vis des clients ayant un accès direct aux comptes de la banque.

Correspondante, et qu'elle soit en mesure de fournir des données d'identification pertinentes sur ces clients sur demande de la banque correspondante.

Recommandation 8

Les institutions financières devraient apporter une attention particulière aux menaces de blanchiment de capitaux inhérentes aux technologies nouvelles ou en développement qui risquent de favoriser l'anonymat, et prendre des mesures supplémentaires, si nécessaire, pour éviter l'utilisation de ces technologies dans les dispositifs de blanchiment de capitaux. Les institutions financières devraient notamment mettre en place des dispositifs de gestion des risques spécifiques liés aux relations d'affaires ou aux transactions qui n'impliquent pas la présence physique des parties.

Recommandation 9

Les pays peuvent autoriser les institutions financières à recourir à des intermédiaires ou à des tiers pour s'acquitter des éléments (a) à (c) des mesures de vigilance relatives à la clientèle ou pour jouer le rôle d'apporteur d'affaires, à condition que les critères précisés ci-après soient respectés. Lorsque un tel recours est autorisé, la responsabilité finale de l'identification du client et de la vérification pèse sur l'institution financière ayant eu recours au tiers.

Les critères qui devraient être respectés sont les suivants :

a) Une institution financière ayant recours à un tiers doit immédiatement obtenir les informations nécessaires concernant les éléments (a) à (c) des mesures de vigilance relatives à la clientèle. Les institutions financières devraient prendre les mesures adéquates pour s'assurer que le tiers est à même de fournir, sur demande et dans les délais les plus brefs, des copies des données d'identification et autres documents pertinents liés au devoir de vigilance relatif à la clientèle.

b) L'institution financière devrait s'assurer que le tiers est soumis à une réglementation et fait l'objet d'une surveillance, et qu'il a pris les mesures visant à se conformer aux mesures de vigilance relatives à la clientèle, conformément aux Recommandations 5 et 10.

Il incombe à chaque pays de décider dans quels pays le tiers qui se conforme aux critères peut être établi, compte tenu des informations disponibles sur les pays qui n'appliquent pas ou appliquent insuffisamment les Recommandations du GAFI.

Recommandation 10

Les institutions financières devraient conserver, pendant au moins cinq ans, toutes les pièces nécessaires se rapportant aux transactions effectuées, à la fois nationales et internationales, afin de leur permettre de répondre rapidement aux demandes d'information des autorités compétentes. Ces pièces doivent permettre de reconstituer les transactions individuelles (y compris, le cas échéant, les montants et les types de devises en cause) de façon à fournir, si nécessaire, des preuves en cas de poursuites pénales.

Les institutions financières devraient conserver une trace écrite des données d'identification obtenues au titre des mesures de vigilance (par exemple, copies ou enregistrement des documents officiels tels que les passeports, les cartes d'identité, les permis de conduire ou des documents similaires), les livres de comptes et la correspondance commerciale pendant cinq ans au moins après la fin de la relation d'affaires.

Les données d'identification et les pièces se rapportant aux transactions devraient être mises à disposition des autorités nationales compétentes pour l'accomplissement de leur mission.

Recommandation 11

Les institutions financières devraient apporter une attention particulière à toutes les opérations complexes, d'un montant anormalement élevé et à tous les types inhabituels de transactions, lorsqu'elles n'ont pas d'objet économique ou licite apparent. Le contexte et l'objet de telles opérations devraient être examinés, dans la mesure du possible; les résultats de cet examen devraient être établis par écrit, et être mis à disposition des autorités compétentes et des commissaires aux comptes.

Recommandation 12

Le devoir de vigilance relatif à la clientèle et de conservation des documents découlant des Recommandations 5, 6, 8 à 11 s'appliquent aux entreprises et professions non financières désignées, dans les circonstances suivantes :

a) Casinos - lorsque les clients effectuent des transactions financières égales ou supérieures au seuil désigné applicable.

b) Agents immobiliers - lorsqu'ils effectuent des transactions pour leurs clients concernant l'achat et la vente de biens immobiliers.

c) Négociants en métaux précieux ou en pierres précieuses - lorsqu'ils effectuent avec un client des transactions en espèces dont le montant est égal ou supérieur au seuil désigné applicable.

d) Avocats, notaires, autres professions juridiques indépendantes et comptables - lorsqu'ils préparent ou effectuent des transactions pour leurs clients dans le cadre des activités suivantes :

- achat et vente de biens immobiliers ;
- gestion des capitaux, des titres ou autres actifs du client ;
- gestion de comptes bancaires, d'épargne ou de titres ;
- organisation des apports pour la création, l'exploitation ou la gestion de sociétés ;
- création, exploitation ou gestion de personnes morales ou de constructions juridiques, et achat et vente d'entités commerciales.

e) Prestataires de services aux sociétés et trusts - lorsqu'ils préparent ou effectuent des transactions pour un client dans le cadre des activités visées par les définitions figurant dans le Glossaire.

Déclaration d'opérations suspectes et conformité

Recommandation 13

Si une institution financière soupçonne ou a des raisons suffisantes de soupçonner que des fonds proviennent d'une activité criminelle, ou sont liés au financement du terrorisme, elles devraient être tenues, directement en vertu d'une loi ou d'une réglementation, de faire sans délai une déclaration d'opérations suspectes auprès de la cellule de renseignements financiers (CRF).

Recommandation 14

Les institutions financières, leurs dirigeants et employés devraient être :

a) Protégés par des dispositions légales contre toute responsabilité, pénale ou civile pour violation des règles de confidentialité- qu'elles soient imposées par contrat ou par toute disposition législative, réglementaire ou administrative- s'ils déclarent de bonne foi leurs soupçons à la CRF, même s'ils ne savaient pas précisément quelle était l'activité criminelle en question, et même si l'activité illégale ayant fait l'objet du soupçon ne s'est pas réellement produite.

b) Soumis à une interdiction légale de divulguer le fait qu'une déclaration d'opérations suspectes ou une information qui la concerne est communiquée à une CRF.

Recommandation 15

Les institutions financières devraient mettre au point des programmes de lutte contre le blanchiment de capitaux et le financement du terrorisme. Ces programmes devraient comprendre :

a) Des politiques, des procédures et des contrôles internes, y compris des dispositifs de contrôle de la conformité et des procédures appropriées lors de l'embauche des employés, de façon à s'assurer qu'elle s'effectue selon des critères exigeants.

b) Un programme de formation continue des employés.

c) Un dispositif de contrôle interne pour vérifier l'efficacité du système.

Recommandation 16

Les obligations découlant des Recommandations 13 à 15, et 21 s'appliquent aux entreprises et professions non financières désignées, avec les précisions suivantes :

a) Les avocats, notaires, autres professions juridiques indépendantes et comptables devraient être tenus de déclarer les opérations suspectes lorsque, pour le compte de ou pour un client, ils effectuent une transaction financière dans le cadre des activités visées par la Recommandation 12(d). Les pays sont fortement encouragés à étendre l'obligation de déclaration à toutes les autres activités professionnelles des comptables, notamment l'activité de vérification des comptes.
b) Les négociants en métaux précieux ou en pierres précieuses devraient être tenus de déclarer les opérations suspectes lorsqu'ils effectuent avec un client des transactions en espèces égales ou supérieures au seuil désigné applicable.

c) Les prestataires de services aux sociétés et trusts devraient être tenus de déclarer les opérations suspectes lorsque, pour le compte de ou pour un client, ils effectuent une transaction s'inscrivant dans le cadre des activités visées par la Recommandation 12(e).

Les avocats, les notaires, les autres professions juridiques indépendantes et les comptables agissant en qualité de juristes indépendants ne sont pas tenus de déclarer les opérations suspectes si les informations qu'ils détiennent ont été obtenues dans des circonstances relevant du secret professionnel ou d'un privilège professionnel légal. (Voir les notes interprétatives pour la Recommandations 16 et pour les Recommandations 5, 12 et 16)

Autres mesures de dissuasion concernant le blanchiment de capitaux et le financement du terrorisme

Recommandation 17

Les pays devraient s'assurer qu'ils disposent de sanctions efficaces, proportionnées et dissuasives, qu'elles soient pénales, civiles ou administratives, applicables aux personnes physiques ou morales

visées par ces Recommandations qui ne se conforment pas aux obligations en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme.

Recommandation 18

Les pays ne devraient pas autoriser l'établissement de banques fictives ni tolérer la poursuite de leurs activités sur leur territoire. Les institutions financières devraient refuser de nouer ou de poursuivre une relation de correspondant bancaire avec des banques fictives. Les institutions financières devraient également se garder de nouer des relations avec des institutions financières clientes étrangères qui autorisent des banques fictives à utiliser leurs comptes.

Recommandation 19

Les pays devraient envisager la faisabilité et l'utilité d'un système par lequel les banques et les autres institutions financières et intermédiaires déclareraient toutes les transactions nationales et internationales en espèces supérieures à un certain montant à une agence centrale nationale disposant d'une base de données informatisée, accessible aux autorités compétentes dans les affaires de blanchiment de capitaux ou de financement du terrorisme, et son utilisation strictement limitée. *(Modifié le 22 octobre 2004)*

Recommandation 20

Les pays devraient envisager d'appliquer les Recommandations du GAFI aux entreprises et professions autres que les entreprises et professions non financières désignées qui présentent des risques au regard du blanchiment de capitaux ou du financement du terrorisme.

Les pays devraient encourager davantage le développement de techniques modernes et sûres de gestion des fonds qui soient moins vulnérables au blanchiment de capitaux.

Mesures à prendre à l'égard des pays qui n'appliquent pas ou appliquent insuffisamment les Recommandations du GAFI

Recommandation 21

Les institutions financières devraient prêter une attention particulière à leurs relations d'affaires et à leurs transactions avec des personnes physiques et morales, notamment des entreprises et des institutions financières, résidant dans les pays qui n'appliquent pas ou appliquent insuffisamment les Recommandations du GAFI. Lorsque ces transactions n'ont pas d'objet économique ou licite apparent, leur contexte et objet devraient, dans la mesure du possible, être examinés et les résultats consignés par écrit et mis à la disposition des autorités compétentes. Si un tel pays persiste à ne pas appliquer ou à appliquer insuffisamment les Recommandations du GAFI, les pays devraient être à même d'appliquer des contre-mesures adaptées.

Recommandation 22

Les institutions financières devraient s'assurer que les principes applicables aux institutions financières susmentionnées sont également appliqués par leurs succursales et leurs filiales majoritairement contrôlées situées à l'étranger, particulièrement dans les pays qui n'appliquent pas ou appliquent insuffisamment les Recommandations du GAFI, dans la mesure où les lois et règlements locaux le permettent. Lorsque ces mêmes lois et règlements s'y opposent, les autorités compétentes du pays où est située la société mère devraient être informées par les institutions financières, que celles-ci ne peuvent appliquer les Recommandations du GAFI.

Réglementation et surveillance

Recommandation 23

Les pays devraient s'assurer que les institutions financières font l'objet d'une réglementation et d'une surveillance adaptées et qu'elles mettent effectivement en œuvre les Recommandations du GAFI. Les autorités compétentes devraient prendre les mesures législatives ou réglementaires nécessaires pour empêcher les criminels ou leurs complices de prendre le contrôle d'institutions financières, d'en être les bénéficiaires effectifs, d'y acquérir une participation significative ou de contrôle, ou d'y occuper un poste de direction.

Pour les institutions financières soumises aux Principes fondamentaux, les mesures réglementaires et de surveillance applicables à des fins prudentielles et qui sont pertinentes aussi en matière de blanchiment de capitaux devraient de manière semblable s'appliquer à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Les autres institutions financières devraient être soumises à une autorisation préalable ou à un enregistrement, faire l'objet d'une réglementation adaptée, et être soumises à une surveillance ou à un contrôle à des fins de lutte contre le blanchiment de capitaux, en fonction du risque de blanchiment de capitaux ou du financement du terrorisme dans ce secteur. Les entreprises prestataires de services de transmission de fonds ou de valeurs, ou de services de change devraient au minimum être soumises à une autorisation préalable ou à un enregistrement, et soumises à des systèmes efficaces de suivi et de contrôle du respect des obligations nationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Recommandation 24

Les entreprises et les professions non financières désignées devraient être soumises aux mesures de réglementation et de surveillance suivantes :

a) Les casinos devraient être soumis à un régime complet de réglementation et de surveillance visant à s'assurer qu'ils ont effectivement pris les mesures nécessaires pour lutter contre le blanchiment et le financement du terrorisme. Au minimum :

- les casinos devraient être soumis à une autorisation préalable ;

les autorités compétentes devraient prendre les mesures législatives ou réglementaires nécessaires pour empêcher les criminels ou leurs complices de prendre le contrôle d'un casino, d'en devenir les bénéficiaires effectifs, d'y acquérir une participation significative ou de contrôle, ou d'y occuper un

- poste de direction ou d'exploitant;
- les autorités compétentes devraient s'assurer que le respect par les casinos de leurs obligations en matière de lutte contre le blanchiment de capitaux et de financement du terrorisme fait l'objet d'une surveillance effective.

b) Les pays devraient s'assurer que les autres catégories d'entreprises et de professions non financières désignées sont soumises à des dispositifs efficaces de suivi et de contrôle du respect de leurs obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Ces mesures devraient être prises en fonction de la sensibilité aux risques. Ces contrôles peuvent être effectués par une autorité gouvernementale ou par une organisation d'autorégulation appropriée, à condition qu'une telle organisation puisse s'assurer que ses membres se conforment à leurs obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Recommandation 25

Les autorités compétentes devraient établir des lignes directrices et assurer un retour de l'information qui aidera les institutions financières et les entreprises et professions non financières désignées à appliquer les mesures nationales de lutte contre le blanchiment des capitaux et le financement du terrorisme, et notamment à détecter et déclarer les opérations suspectes.

MESURES INSTITUTIONNELLES ET AUTRES MESURES NECESSAIRES DANS LES SYSTEMES DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

Les autorités compétentes, leurs attributions et leurs ressources

Recommandation 26

Les pays devraient mettre en place une CRF qui serve de centre national pour recueillir (et, dans les cas prévus, de solliciter), analyser et transmettre les déclarations d'opérations suspectes et d'autres informations concernant les actes susceptibles d'être constitutifs de blanchiment de capitaux et de financement du terrorisme. La CRF devrait avoir accès, directement ou indirectement et en temps voulu, aux informations financières, administratives et en provenance des autorités de poursuite pénale pour exercer correctement ses fonctions et notamment analyser les déclarations d'opérations suspectes.

Recommandation 27

Les pays devraient s'assurer que les enquêtes sur le blanchiment de capitaux et le financement du terrorisme sont confiées à des autorités de poursuite pénale spécifiques. Les pays sont encouragés à soutenir et à développer, autant que possible, les techniques d'enquêtes spécifiques adaptées aux enquêtes sur le blanchiment de capitaux, comme la livraison surveillée, les opérations sous couverture et autres techniques pertinentes. Les pays sont également encouragés à utiliser d'autres mécanismes efficaces tels que le recours à des groupes permanents ou temporaires spécialisés dans les enquêtes sur les biens, et les enquêtes menées en coopération avec les autorités compétentes appropriées d'autres pays.

Recommandation 28

Lorsqu'elles se livrent à des enquêtes sur le blanchiment de capitaux et les infractions sous-jacentes, les autorités compétentes devraient pouvoir obtenir des documents et des informations pour les utiliser dans le cadre de ces enquêtes et pour engager les poursuites et actions qui s'y rapportent. Ceci inclut le pouvoir d'appliquer des mesures coercitives pour la production de documents détenus par des institutions financières ou d'autres personnes, pour la fouille de personnes et de locaux et pour la saisie et l'obtention d'éléments de preuve.

Recommandation 29

Les autorités de surveillance devraient être dotées des pouvoirs nécessaires pour contrôler et s'assurer que les institutions financières respectent leurs obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, et notamment du pouvoir de procéder à des inspections. Ces autorités devraient être autorisées à exiger des institutions financières la délivrance de toute information ayant trait au contrôle du respect de leurs obligations et à imposer des sanctions administratives adaptées en cas de non respect de ces obligations.

Recommandation 30

Les pays devraient doter leurs autorités compétentes impliquées dans la lutte contre le blanchiment de capitaux et le financement du terrorisme de ressources financières, humaines et techniques adéquates. Les pays devraient mettre en place des procédures visant à garantir la plus haute intégrité du personnel de ces autorités.

Recommandation 31

Les pays devraient faire en sorte que les responsables de l'action gouvernementale, la CRF, les autorités de poursuite pénale et les autorités de surveillance disposent de mécanismes efficaces leur permettant de coopérer, et, le cas échéant, de coordonner leur action au plan national en ce qui concerne l'élaboration et la mise en oeuvre de politiques et d'activités de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Recommandation 32

Les pays devraient faire en sorte que leurs autorités compétentes puissent examiner l'efficacité de leurs systèmes de lutte contre le blanchiment de capitaux et le financement du terrorisme en tenant des statistiques complètes sur des questions relatives à l'efficacité et au bon fonctionnement de ces systèmes. Ces statistiques devraient porter sur les déclarations d'opérations suspectes reçues et diffusées ; les enquêtes ; les poursuites et condamnations liées au blanchiment de capitaux et au financement du terrorisme ; les biens gelés, saisis ou confisqués ; et l'entraide judiciaire ou les autres demandes internationales de coopération.

Transparence des personnes morales et constructions juridiques

Recommandation 33

Les pays devraient prendre des mesures pour empêcher l'utilisation illicite de personnes morales par les blanchisseurs de capitaux. Les pays devraient s'assurer que des informations adéquates, pertinentes et à jour sur les bénéficiaires effectifs et sur le contrôle des personnes morales peuvent être obtenues ou consultées en temps voulu par les autorités compétentes. En particulier, les pays dans lesquels les personnes morales peuvent émettre des actions au porteur devraient prendre les mesures appropriées pour faire en sorte que ces personnes ne soient pas utilisées à mauvais escient pour blanchir des capitaux, et devraient être capables de démontrer l'adéquation de ces mesures. Les pays pourraient envisager de prendre des mesures pour faciliter l'accès aux informations sur les bénéficiaires effectifs et sur le contrôle des personnes morales, nécessaires aux institutions financières pour se conformer aux obligations découlant de la Recommandation 5.

Recommandation 34

Les pays devraient prendre des mesures pour empêcher l'utilisation illicite de constructions juridiques par les blanchisseurs de capitaux. Les pays devraient notamment s'assurer que des informations adéquates, pertinentes et à jour sur les trusts exprès, notamment des informations sur les personnes ayant constitué ces trusts exprès, les administrateurs et les bénéficiaires, peuvent être obtenues ou consultées en temps voulu par les autorités compétentes. Les pays pourraient envisager de prendre des mesures pour faciliter l'accès aux informations sur les bénéficiaires effectifs et sur le contrôle des constructions juridiques, nécessaires aux institutions financières pour se conformer aux obligations découlant de la Recommandation 5.

COOPÉRATION INTERNATIONALE

Recommandation 35

Les pays devraient prendre des mesures immédiates pour devenir parties et mettre en œuvre sans restriction la Convention de Vienne, la Convention de Palerme, et la Convention internationale des Nations Unies de 1999 pour la Répression du Financement du Terrorisme. Les pays sont également encouragés à ratifier et mettre en œuvre d'autres conventions internationales appropriées telles que la Convention

Du Conseil de l'Europe de 1990 sur le Blanchiment de Capitaux, la Recherche, la Saisie et la Confiscation des Produits du Crime et la Convention Interaméricaine de 2002 contre le Terrorisme.

Entraide judiciaire et extradition

Recommandation 36

Les pays devraient offrir rapidement, efficacement et d'une manière constructive, l'éventail le plus large possible de mesures d'entraide judiciaire pour les enquêtes, les poursuites et les procédures connexes ayant trait au blanchiment de capitaux et au financement du terrorisme. En particulier, les pays :

a) Ne devraient pas interdire ou assortir de conditions déraisonnables ou indûment restrictives l'octroi de l'entraide judiciaire.

b) Devraient faire en sorte d'avoir des procédures claires et efficaces d'exécution des demandes d'entraide judiciaire.

c) Ne devraient pas refuser d'exécuter une demande d'entraide judiciaire pour l'unique motif que l'infraction est également considérée comme portant sur des questions fiscales.

d) Ne devraient pas refuser d'exécuter une demande d'entraide judiciaire au motif que leurs lois imposent aux institutions financières la préservation du secret ou de la confidentialité.

Les pays devraient faire en sorte que les pouvoirs dont leurs autorités compétentes doivent disposer, conformément à la Recommandation 28, puissent également être utilisés en réponse à une demande d'entraide judiciaire et, si cela est conforme à leur dispositif interne, en réponse à une demande directe adressée par des autorités judiciaires ou de poursuite pénale étrangères à leurs homologues nationaux.

Afin d'éviter les conflits de compétence, il conviendrait d'étudier la possibilité d'élaborer et de mettre en œuvre des mécanismes permettant de déterminer, dans l'intérêt de la justice, le lieu de

saisine le plus approprié pour les poursuites de personnes mises en cause dans des affaires sujettes à des poursuites dans plusieurs pays.

Recommandation 37

Les pays devraient dans toute la mesure du possible s'accorder l'entraide judiciaire même en l'absence de double incrimination

Lorsque la double incrimination est exigée pour l'entraide judiciaire ou l'extradition, cette obligation devrait être considérée comme remplie, que les deux pays classent ou non l'infraction dans la même catégorie d'infractions ou qu'ils utilisent ou non la même terminologie pour la désigner, dès lors que les deux pays incriminent l'acte qui est à la base de l'infraction.

Recommandation 38

Il serait souhaitable que des mesures rapides puissent être prises en réponse à des requêtes émanant de pays étrangers demandant d'identifier, de geler, de saisir et de confisquer des biens blanchis, les produits d'opérations de blanchiment ou d'infractions sous-jacentes, les instruments utilisés ou destinés à être utilisés pour commettre ces infractions ou des biens d'une valeur équivalente. De même, il devrait exister des mesures visant à coordonner les procédures de saisie et de confiscation, pouvant inclure le partage des avoirs confisqués.

Recommandation 39

Les pays devraient reconnaître le blanchiment de capitaux comme une infraction pouvant donner lieu à extradition. Chaque pays devrait soit extrader ses propres nationaux, soit, lorsque le pays ne le fait pas uniquement pour des raisons de nationalité, devrait, à la demande du pays requérant l'extradition, soumettre l'affaire sans tarder à ses autorités compétentes afin que des poursuites soient engagées à l'égard des infractions mentionnées dans la demande. Ces autorités devraient prendre leurs décisions et conduire leurs procédures comme ils le feraient pour toute autre infraction grave dans le cadre de leur droit interne. Les pays concernés devraient coopérer, en particulier pour les aspects concernant la procédure et la preuve, afin d'assurer l'efficacité de ces poursuites.

Sous réserve que leurs systèmes juridiques le permettent, les pays pourraient envisager de simplifier l'extradition en autorisant la transmission directe des demandes d'extradition entre les ministères compétents, l'extradition des personnes sur le seul fondement d'un mandat d'arrêt ou d'un jugement et/ou l'extradition simplifiée des personnes acceptant de renoncer à la procédure formelle d'extradition.

Autres formes de coopération

Recommandation 40

Les pays devraient faire en sorte que leurs autorités compétentes accordent à leurs homologues étrangers la coopération internationale la plus large possible. Il conviendrait que soient mis en place des dispositifs clairs et efficaces pour faciliter un échange rapide et constructif directement entre les homologues de chaque pays, spontanément ou sur demande, des informations ayant trait aussi bien au blanchiment de capitaux qu'aux infractions sous-jacentes. Ces échanges devraient être autorisés sans condition indûment restrictive. En particulier :

a) Les autorités compétentes ne devraient pas refuser une demande d'entraide au seul motif que la demande est également considérée comme portant sur des questions fiscales.

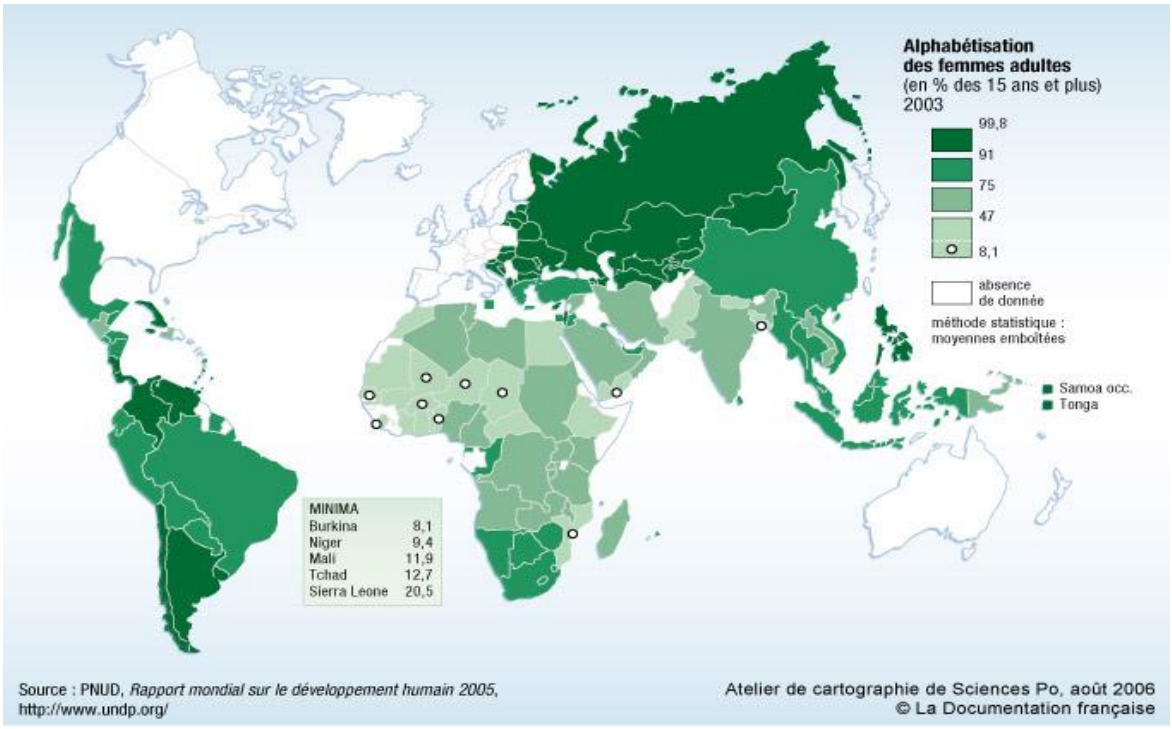
b) Les pays ne devraient pas, pour refuser la coopération, invoquer les lois qui imposent aux institutions financières de préserver le secret ou la confidentialité.

c) Les autorités compétentes devraient pouvoir exécuter des demandes d'informations et, si possible, procéder à des enquêtes, pour le compte d'homologues étrangers.

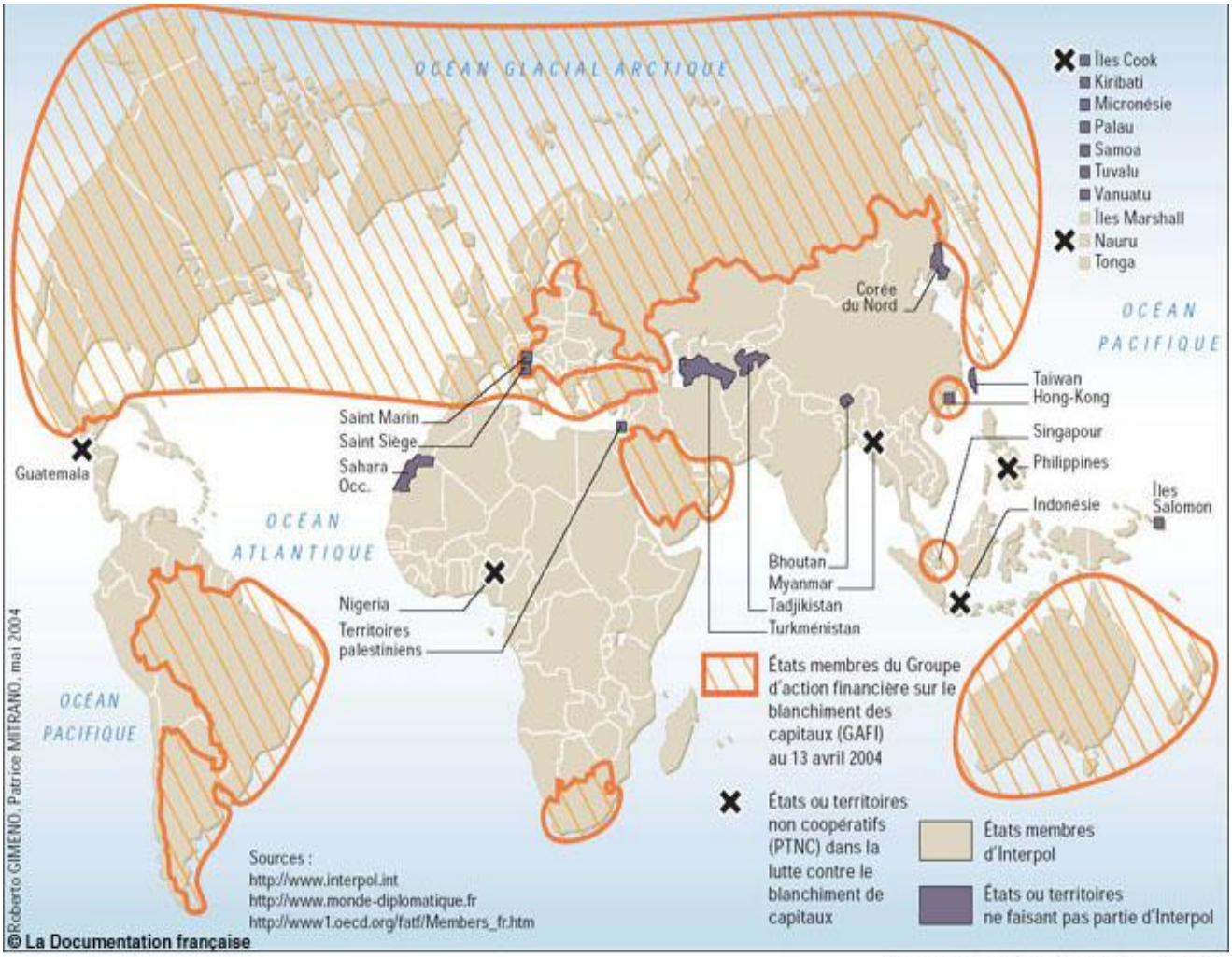
Lorsque la possibilité d'obtenir des informations recherchées par une autorité compétente étrangère ne fait pas partie des prérogatives de l'autorité homologue, les pays sont également encouragés à permettre un échange rapide et constructif d'informations avec les autorités non homologues. La coopération avec les autorités étrangères autres que les autorités homologues pourrait avoir lieu directement ou indirectement. Lorsqu'elles ont un doute quant à la démarche à suivre, les autorités compétentes devraient d'abord contacter leurs homologues étrangers pour qu'ils leur prêtent assistance.

Les pays devraient mettre en place des contrôles et des garanties pour faire en sorte que les informations échangées par les autorités compétentes ne soient utilisées que de la manière autorisée et en conformité avec leurs obligations de protection de la vie privée et de protection des données.

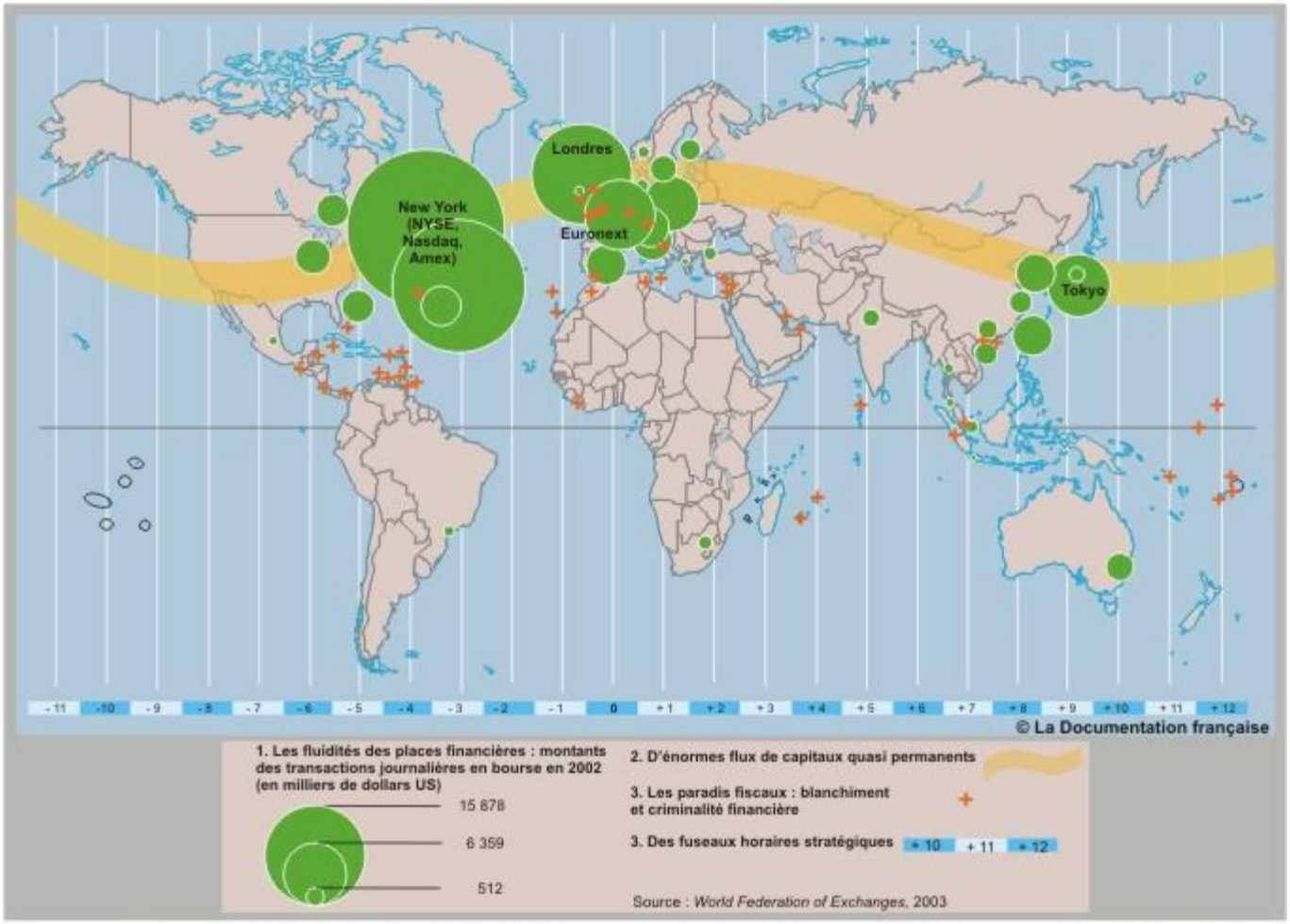
Annexe C



Alphabétisation des femmes adultes en 2003 — Source : Documentation photographique n°8053



Source : Questions internationales n° 8



MONDE - Mobilité géographique du capital financier international (2002) Source : Documentation photographique, n°8037

BIBLIOGRAPHIE

Des sites internet

-Www. fatf.org /

-http://www.carleton.ca/cciss/res-doc /itac/samy-f.pdf

-http://europa.eu/scadplus/leg /fr/lvb/133254 .htm

- http://www.investigateur.info/news/articles/articl-financiers-terror.htlm

- http:/menaceterroriste.free.fr/reseaux-financiers.htm

- http://www.infosentinel;com/info/news-22.htm

- http://www.xerion-finance.com/lettre-information.php

- http://agora.qc.ca/mot.nsf/dossier/terrorisme

- http://europa.eu/scadplus/leg /fr/s22008.htm

- http://www.terrorisme:net/doc/etudes2002

- http://www.terrorisme:net/p/article-154.shmi

Des ouvrages

-**La mécanique terroriste**, Bruce Hoffman, éd. Calmann-Lévy 2000.

-**Histoire mondiale du terrorisme**, Gérard Chalian.

-Les volontaires de la mort : l'arme du suicide, François Géré 2003

-**Blanchiment et financement du terrorisme**, Ludovic François, pascal CHAIGNEAU, Marc CHESNEY, 2004.

-**Qui finance le terrorisme international?** Loretta Napoleoni.

-**Au nom d' Oussama ben Laden …**Ronald jacquard 2001

-**l'argent de la terreur** jean- Luc Peduzzi, 2006.

- **Academey & finance** deuxième forum de genève sur le crime organisé 2006.

- **L'arme du terrorisme** Chaliand G /Audibdibert 2003

-**La guerre asymétrique** Braud P/Le Roucher 2002

Table des matières

Mémoire de géopolitique

Terrorisme et géopolitique

Résume de Mémoire (Modes de financement du terrorisme)

1. Terrorisme et géopolitique, modes de financement du terrorisme
2. Lieutenant Colonel, armée de Terre, AMER Ahmed, EGYPTE
3. 12 mars 2007
4. Division B – groupe B2
5. Mémoire de Géopolitique

6- Mots clés : terrorisme, financement, blanchement, cyber-terroriste, explosives.

7- Le mot **terrorisme** est employé pour la première fois après la Révolution Française. Il se rapportait au régime de **La Terreur** Mais les phénomènes que l'on connaît aujourd'hui sous le nom de terrorisme sont bien différents. Désormais, on appelle terrorisme une stratégie de lutte, de guerre, que choisit le plus faible pour combattre un adversaire plus fort militairement.

Les guerres sont nombreuses et les exemples de terrorisme aussi : Irlande du Nord, Corse. De quoi s'agit-il ? De groupes de personnes, politiquement organisés, qui décident de faire des **attentats**, c'est-à-dire des actions violentes contre des personnes ou des biens appartenant à leur ennemi déclaré. Le terrorisme est une stratégie pour rendre visible un état de guerre qui parfois ne l'est pas. C'est une forme de guerre en fait.

Et, parce que ce sont des cibles plus faciles à toucher, les objectifs des attentats peuvent parfois être des civils, de simples citoyens de l'Etat contre lequel les terroristes sont en guerre.

Le terrorisme est une façon de démontrer que la guerre existe ou d'attirer l'attention sur des désirs de changement. Les terroristes utilisent donc la violence la plus visible possible, pour faire peur à leur ennemi. Souvent ils espèrent que la terreur de la population contraindra leur adversaire à négocier avec eux ou à changer d'attitude. Les terroristes défendent des causes, des idéaux, parfois justes au travers d'actions terribles, injustifiables (comme toute guerre).

Le blanchiment de capitaux et le financement du terrorisme soulèvent de gros problèmes en matière de prévention, de détection et de poursuite pour une grande partie des pays.

Les techniques sophistiquées utilisées pour blanchir des capitaux ou financer le terrorisme rendent ces problèmes plus complexes encore.

Ces techniques sophistiquées peuvent impliquer différents types d'institutions financières ; de nombreuses transactions financières utilisant plusieurs institutions financières ou d'autres organismes tels que des conseillers financiers, des sociétés-écrans et des fournisseurs de services comme intermédiaires ; des transferts, via et vers différents pays ; et l'utilisation de nombreux instruments financiers et autres types d'actifs à accumulation de valeur. Le blanchiment de capitaux est toutefois un concept assez simple.

Il s'agit d'un procédé par lequel le produit d'une activité criminelle est déguisé pour cacher son origine illicite. Au fond, le blanchiment de capitaux concerne davantage le *produit* de biens d'origine criminelle que les biens eux-mêmes.

Le financement du terrorisme est également un concept simple à la base.

Il s'agit du soutien financier, quelle qu'en soit la forme, du terrorisme ou de ceux qui le soutiennent, le planifient ou le commettent.

Il est toutefois moins facile de définir le terrorisme lui-même car le terme peut avoir d'importantes implications politiques, religieuses et nationales qui diffèrent d'un pays à l'autre.

Le blanchiment de capitaux et le financement du terrorisme présentent souvent des caractéristiques transactionnelles similaires, la plupart étant liées à la dissimulation.

Les blanchisseurs de capitaux envoient des fonds illicites par des voies légales afin de cacher l'origine criminelle de ceux-ci alors que les personnes qui financent le terrorisme transfèrent des fonds qui peuvent avoir une origine légale ou illicite de manière à cacher leur origine et leur utilisation finale, qui est le soutien au terrorisme.

Le résultat est cependant le même : la récompense.

Une fois les capitaux blanchis, les criminels sont récompensés par un produit déguisé et apparemment légitime.

De même, ceux qui financent le terrorisme sont récompensés en apportant un soutien financier visant à mettre en place des stratagèmes et des attaques terroristes.

Ma mémoire est devisée en deux parties :

La première partie est un aperçu sur le terrorisme, qui contiennent **la définition, l'origine, la motivation du terrorisme.**

Méthodes du terrorisme :

a) les méthodes qui visent les biens (attentats à la bombe contre des bâtiments et des véhicules).

b) les méthodes qui sont dirigées contre des personnes et leur liberté (les prises d'otage) ou leur intégrité physique (assassinats sous diverses formes).

c) les méthodes qui frappent à la fois les personnes et les biens matériels (les détournements d'aéronefs).

Le cyber-terrorisme :

-Qu'est-ce que le cyber-terrorisme ?

- Qu'est-ce que le cyber-terrorisme ?

- Les armes des cyber-terroristes.

- Les communications, le recrutement et la formation.

- L'avenir de cyber-terrorisme.

La menace chimique.

Après les attentats du 11 septembre 2001 :

1-Conséquences dans les rapports internationaux.
- -Une remise en cause de l'uni polarité
- -Une nouvelle remise en cause de la politique étrangère des Etats-Unis
- - Un changement dans le règlement des conflits du Moyen-Orient
- -Une analyse critique de l'action militaire américaine
- -Des relations interreligieuses plus difficiles

2-Conséquences économiques
- - Sur le transport aérien
- - Sur le commerce du tourisme international
- -Sur les relations bancaires internationales

3- Conséquences juridiques

Dans la 2eme partie j'ai parlé des ressources d'activités terroristes, qui contiennent **les différentes sources de financement terroristes :**

-Étatiques (états dévoyés-états escroqués-états en contexte de conflit armé)

- À légalité variable (don de particuliers-organismes humanitaires-cotisations-vente de publication/marchandises)

- Illégales (activités criminelles organisées- enlèvements- extorsions -contrebande-fraudes - soutien financier des militants et des diasporas (L' E.T.A au pays Basque ou l'I.R.A en Irlande) - l'impôt révolutionnaire, qui prend en fait la forme de racket organisé, essentiellement auprès des entreprises (les sociétés d'import-export sont très pratiques pour les mouvements de fonds et de matériel par exemple).

Les transferts de fonds

- Les systèmes informels de transfert de fonds

- Définitions et terminologies : des lectures partielles

- Une continuité séculaire

-Des systèmes adaptés à une population émigrante

-Des liens forts entre les participants

- Une réponse aux coûts élevés des banques

- Les transferts de fonds et le financement d'activités terroristes

- L'attrait des systèmes informels de transfert de fonds : pas de trace de papier

- Les terroristes utilisent également les systèmes bancaires officiels

-L'obligation de divulguer les opérations douteuses : un sujet de controverse parmi les acteurs

Blanchiment d'argent et financement du terrorisme : conjonctures nationales

-L'obligation de divulguer les opérations douteuses : un sujet de controverse parmi les acteurs

-Blanchiment d'argent et dynamiques spécifiques des groupes terroristes

-Distinguer entre « blanchiment d'argent » (un délit passé) et « financement du terrorisme » (une activité future)

- Utilisation du réseau bancaire officiel et des systèmes de transfert de fonds : les groupes terroristes ont accès à des sources légitimes de revenus

- Les procédés de blanchiment d'argent des groupes terroristes recoupent en partie ceux des organisations criminelles

FICHE DOCUMENTAIRE

1. Terrorisme et géopolitique, modes de financement du terrorisme
2. Lieutenant Colonel, armée de Terre, AMER Ahmed, EGYPTE
3. 12 mars 2007
4. Division B – groupe B2
5. Mémoire de Géopolitique

6. Mots clés financement, blanchement, terrorisme.

7. Le blanchiment de capitaux et le financement du terrorisme soulèvent de gros problèmes en matière de prévention, de détection et de poursuite pour une grande partie des pays.

Les techniques sophistiquées utilisées pour blanchir des capitaux ou financer le terrorisme rendent ces problèmes plus complexes encore.

Ces techniques sophistiquées peuvent impliquer différents types d'institutions financières ; de nombreuses transactions financières utilisant plusieurs institutions financières ou d'autres organismes tels que des conseillers financiers, des sociétés-écrans et des fournisseurs de services comme intermédiaires ; des transferts, via et vers différents pays ; et l'utilisation de nombreux instruments financiers et autres types d'actifs à accumulation de valeur. Le blanchiment de capitaux est toutefois un concept assez simple.

Il s'agit d'un procédé par lequel le produit d'une activité criminelle est déguisé pour cacher son origine illicite. Au fond, le blanchiment de capitaux concerne davantage le *produit* de biens d'origine criminelle que les biens eux-mêmes.

Le financement du terrorisme est également un concept simple à la base.

Il s'agit du soutien financier, quelle qu'en soit la forme, du terrorisme ou de ceux qui le soutiennent, le planifient ou le commettent.

Il est toutefois moins facile de définir le terrorisme lui-même car le terme peut avoir d'importantes implications politiques, religieuses et nationales qui diffèrent d'un pays à l'autre.

Le blanchiment de capitaux et le financement du terrorisme présentent souvent des caractéristiques transactionnelles similaires, la plupart étant liées à la dissimulation.

Les blanchisseurs de capitaux envoient des fonds illicites par des voies légales afin de cacher l'origine criminelle de ceux-ci alors que les personnes qui financent le terrorisme transfèrent des

fonds qui peuvent avoir une origine légale ou illicite de manière à cacher leur origine et leur utilisation finale, qui est le soutien au terrorisme.

Le résultat est cependant le même : la récompense.

Une fois les capitaux blanchis, les criminels sont récompensés par un produit déguisé et apparemment légitime.

De même, ceux qui financent le terrorisme sont récompensés en apportant un soutien financier visant à mettre en place des stratagèmes et des attaques terroristes.