**Criminologie**

# Les opérations terroristes réseaucentriques

Benoît Gagnon

Volume 39, numéro 1, printemps 2006

Le cybercrime

URI : https://id.erudit.org/iderudit/013124ar
DOI : https://doi.org/10.7202/013124ar

Aller au sommaire du numéro

Éditeur(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (imprimé)
1492-1367 (numérique)

Découvrir la revue

Citer cet article

Gagnon, B. (2006). Les opérations terroristes réseaucentriques. *Criminologie*, *39*(1), 23–42. https://doi.org/10.7202/013124ar

Résumé de l'article

Les travaux effectués sur le terrorisme ont tendance à décrire le phénomène comme un élément statique. Or, pour bien comprendre le terrorisme, il est de notre avis qu'il faut plutôt conduire des analyses plus « biologiques » qui examinent, en juxtaposition, le fonctionnement interne des groupes terroristes et l'environnement dans lequel ils évoluent. Ce texte aura donc pour but de prendre en considération cette dynamique interne/externe. Cela nous permettra de constater que les organisations terroristes contemporaines ont pu créer de nouvelles méthodes de fonctionnement : les opérations réseaucentriques. Ce nouveau mode opérationnel a pour objectif d'accroître l'efficacité de l'organisation terroriste et de lui permettre de mieux faire face au contexte de sécurité actuel. En exploitant le potentiel des technologies de l'information, les groupes terroristes se sont dotés de moyens pour résister aux opérations contre-terroristes.

# Les opérations terroristes réseaucentriques

Benoît Gagnon
*Doctorant, École de criminologie de l'Université de Montréal*
*Chercheur, Chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'UQAM*
*Assistant de recherche, Équipe de recherche sur le terrorisme et l'antiterrorisme au Canada*
*benoit.gagnon@gmail.com*

**RÉSUMÉ** • Les travaux effectués sur le terrorisme ont tendance à décrire le phénomène comme un élément statique. Or, pour bien comprendre le terrorisme, il est de notre avis qu'il faut plutôt conduire des analyses plus « biologiques » qui examinent, en juxtaposition, le fonctionnement interne des groupes terroristes et l'environnement dans lequel ils évoluent. Ce texte aura donc pour but de prendre en considération cette dynamique interne/externe. Cela nous permettra de constater que les organisations terroristes contemporaines ont pu créer de nouvelles méthodes de fonctionnement : les opérations réseaucentriques. Ce nouveau mode opérationnel a pour objectif d'accroître l'efficacité de l'organisation terroriste et de lui permettre de mieux faire face au contexte de sécurité actuel. En exploitant le potentiel des technologies de l'information, les groupes terroristes se sont dotés de moyens pour résister aux opérations contre-terroristes.

**ABSTRACT** • The trend in terrorism studies is to approach the phenomenon as uniform and quite static. We believe that this is an error. We consider that a more "biological" method is necessary to grasp the inner dynamic of terrorist organizations and their interaction with the environment in which they evolve. By taking into account this internal/external relationship, the present analysis will lead us to understand clearly how contemporary terrorists have shifted towards network centric operations. The goals of this new operational framework are to allow terrorist organizations to be more efficient, and to defeat the new security structures. By exploiting the potential of information technologies, terrorists have created new ways to resist to counterterrorist operations.

## Introduction

Depuis que la « guerre » contre le terrorisme a été lancée aux États-Unis, plusieurs analystes en stratégie et en sécurité se questionnent sur les techniques les plus efficaces pour ébranler la nébuleuse d'Al-Qaïda et faire des gains significatifs sur la menace terroriste. Essentiellement axées sur les méthodes antiterroristes classiques, comme celles employées dans la guerre contre le terrorisme irlandais, ces analyses ne tiennent pas compte des changements profonds du système international depuis la fin de la guerre froide.

Le même réflexe est d'ailleurs présent dans bon nombre de travaux universitaires consacrés au sujet. Pour plusieurs auteurs, le terrorisme contemporain ne présente pas de changement dans sa composition. C'est, entre autres, la vision prônée par Pierre Mannoni (2004 : 26) qui soutient que l'attentat terroriste du 11 septembre est « [...] le même terrorisme qui a aussi fauché les victimes des autres attentats. C'est le même phénomène auquel on assiste dans tous les cas de figure. À New York, il a mieux réussi qu'ailleurs son accaparement de la scène médiatique. C'est la principale différence. »

C'est également la vision prônée par d'autres chercheurs, dont Paul Berman, professeur de journalisme à la New York University. Dans son ouvrage *Terror and Liberalism* (2003), l'auteur rejette l'idée d'une transformation du phénomène terroriste. Selon son point de vue, nous sommes face à un terrorisme *pas si nouveau* qui n'est que le résultat d'une évolution normale du phénomène.

De telles affirmations sont, à notre avis, plutôt réductrices. En effet, elles ne prennent pas en considération les transformations qui se sont produites à l'intérieur des organisations terroristes. De même, elles ne se penchent pas sur les répercussions qu'ont les systèmes de sécurité sur les fondements structurels des groupes terroristes. Ce genre d'analyse considère donc les organisations terroristes comme des éléments assez isolés, statiques, figés dans le temps et incapables d'évoluer.

Nous croyons que les groupes terroristes doivent être analysés selon une approche plus *biologique*. Il est illusoire de croire que ces organisations évoluent dans un monde qui n'obéit pas aux mêmes transformations sociopolitiques présentes dans le système international. Comme n'importe quelle autre organisation, le groupe terroriste, en tant que structure humaine, est nécessairement conditionné par les grandes tendances présentes dans la période suivant la guerre froide : la mondialisation, la montée des technologies de l'information et l'affaissement du modèle

étatique. Il est probablement plus juste de considérer que le terrorisme a muté et s'est adapté aux nouvelles réalités sociopolitiques et policières plutôt que de le percevoir comme un phénomène fixe et amorphe.

C'est justement cette adaptation aux nouvelles réalités internationales qui a eu pour effet de faire émerger un nouveau paradigme terroriste. Elle doit évidemment se juxtaposer à une pléiade d'autres facteurs importants, comme la radicalisation de l'islamisme, par exemple. Néanmoins, il est clair que la relation entre les terroristes et leur environnement joue pour beaucoup dans la structuration des activités internes au groupe. En fait, il serait plus approprié de parler de l'interdépendance entre les individus, la dynamique de groupe et l'environnement policier.

Certes, l'attentat du 11 septembre n'est pas l'élément pivot de ce changement paradigmatique, néanmoins, il catalyse plusieurs des éléments marquants d'une nouvelle forme de terrorisme. Les effets sociopsychopolitiques du terrorisme contemporain sont peut-être les mêmes que ceux du terrorisme classique, mais les méthodes et moyens exploités pour en arriver à de tels attentats, eux, sont fondamentalement différents de ce qui se faisait dans le passé.

Soulignons que ce type de raisonnement n'est pas étranger aux travaux portant sur le terrorisme. Comme le soulignent Martin et Romano (1992 : 35-36) dans leur ouvrage *Multinational Crime : Terrorism, Espionage, Drugs & Arms Trafficking*, les études sur le terrorisme présentent généralement trois lacunes importantes. Tout d'abord, elles ne sont pas fondées sur un cadre théorique ou méthodologique approprié. Ensuite, elles présentent généralement très peu de données empiriques sur les modes de fonctionnement internes des groupes terroristes et les relations qu'ils entretiennent avec l'environnement dans lequel ils évoluent. Finalement, ces analyses saisissent habituellement très mal les convictions et les objectifs des groupes terroristes.

Le présent article ne cherchera bien évidemment pas à résoudre les problèmes fondamentaux de la *terrologie*[1]. Néanmoins, nous nous pencherons sur un aspect qui, comme décrit précédemment, est souvent mis de côté dans l'étude du terrorisme, c'est-à-dire le fonctionnement interne des organisations terroristes par rapport à l'environnement dans lequel elles évoluent. Cette analyse cherchera à démontrer que les structures organisationnelles des groupes terroristes contemporains leur permet-

1 Ce terme correspond à l'étude du terrorisme comme phénomène (George, 1991 : 76-101).

tent d'exécuter des opérations plus efficaces, mais que cela se fait aux prix d'une dépendance accrue aux technologies de l'information.

Notre argumentation sera divisée en trois parties. Premièrement, nous verrons comment les terroristes façonnent leurs organisations. Nous discuterons des différentes formes de hiérarchies étant à la disposition des organisations terroristes, et plus précisément les structures réseautiques. Deuxièmement, nous aborderons les possibilités offertes par les organisations en réseau. Ainsi, nous verrons que certaines formes de réseaux permettent d'établir des opérations dites réseaucentriques, c'est-à-dire des opérations qui exploitent de manière efficace les structures en réseau. Cela nous fournira l'occasion de constater que les groupes terroristes employant les opérations réseaucentriques sont désormais dépendants des technologies de l'information pour bien fonctionner. Troisièmement, nous analyserons les failles que présentent les opérations terroristes réseaucentriques. Ces vulnérabilités structurelles représentent des cibles de choix pour les institutions chargées de la sécurité cherchant à déstabiliser les groupes terroristes. Cela nous permettra de dresser une liste non exhaustive des moyens qui sont à la portée des autorités pour contrer efficacement les opérations terroristes réseaucentriques.

## 1. La réseautique terroriste

Le terrorisme est un sujet très complexe qui soulève une importante série de difficultés dans son analyse. Un des obstacles les plus grands tient d'ailleurs à sa définition même. Le concept de terrorisme est flou et aucune définition ne fait consensus à ce jour. Pour le bien de cet article, nous ne rentrerons pas dans le débat sur la définition du phénomène. Nous emploierons plutôt une définition que nous jugeons utile et pouvant être aisément instrumentalisée pour notre analyse. La définition retenue sera celle avancée par l'Organisation des Nations Unies (ONU), son caractère internationaliste ayant influencé ce choix. Sera donc considéré comme terrorisme :

> Tout [...] acte destiné à tuer ou blesser grièvement un civil, ou tout autre personne qui ne participe pas directement aux hostilités dans un conflit armé, lorsque, par sa nature ou son contexte, cet acte vise à intimider ou à contraindre un gouvernement ou une organisation internationale à accomplir ou s'abstenir d'accomplir un acte quelconque (Organisation des Nations Unies, 1999).

Si cette définition illustre un caractère essentiellement fonctionnel, il est clair qu'elle demeure académiquement imprécise. Toutefois, elle nous permet de situer le concept de terrorisme dans le cadre de cet article.

Depuis le milieu des années 1990, les spécialistes de la question du terrorisme, essentiellement les spécialistes états-uniens, soutiennent qu'émerge une nouvelle forme de terrorisme (Combs, 2003 ; Hoffman, 1999 ; Lesser *et al.,* 1999 ; Laqueur, 2000 ; Morgan, 2004). Ce *nouveau terrorisme*[2] aurait des caractéristiques fondamentalement différentes du terrorisme de la précédente génération. De ces caractéristiques, notons les six principales : 1) les attentats perpétrés par les nouveaux terroristes seraient de plus en plus financés par des États, ce qui augmenteraient leurs capacités tactiques et stratégiques ; 2) les nouveaux terroristes seraient plus enclins à employer les armes de destruction massive ; 3) les nouveaux terroristes seraient de plus en plus motivés par des considérations religieuses, notamment celles sous-tendues par l'islamisme radical (Rubin, 2002) ; 4) les nouveaux terroristes ne voudraient plus atteindre des objectifs sociopolitiques, mais chercheraient plutôt à engendrer la destruction et le chaos ; 5) le nouveau terrorisme serait plus mortel ; 6) il y aurait une augmentation considérable des dégâts engendrés par les attentats commis par les terroristes de la nouvelle génération.

La montée du nouveau terrorisme met en évidence une complexification de plus en plus marquée des organisations terroristes. Cette complexification du terrorisme est la conséquence d'une tendance à l'adoption de structures *en réseau* par les groupes terroristes. Dans son ouvrage *Understanding Terror Networks*, Marc Sageman décrit ainsi le fonctionnement des structures terroristes en réseau :

> *A group of people can be viewed as a network, a collection of nodes connected through links. Some nodes are more popular and are attached to more links, connecting them to other more isolated nodes. These more connected nodes, called hubs, are important components of a terrorist network* (Sageman, 2004 : 137).

Les travaux effectués par la RAND, sous l'égide de David Ronfeldt et John Arquilla (Arquilla et Ronfeldt, 2001), semblent d'ailleurs confirmer cette tendance à la *réseautisation* des structures organisationnelles terroristes.

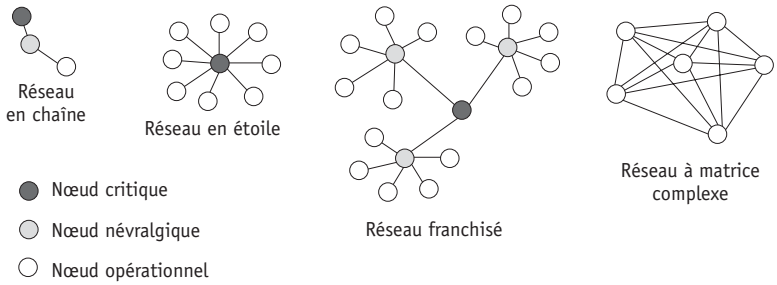
Comme les auteurs le démontrent, il existe différents types de réseaux terroristes. Selon les auteurs, quatre modèles de réseaux peuvent être

---

2 Il faut noter que le concept de *nouveau terrorisme* ne fait pas l'unanimité chez les spécialistes de cette question (Tucker, 2001).

définis : les réseaux en chaîne, les réseaux en étoile, les réseaux franchisés et les réseaux à matrice complexe. Chacun d'entre eux comporte des avantages et des inconvénients. Dans les modèles proposés par les auteurs, on voit que l'importance stratégique des nœuds (*nodes*) réseautiques varie en fonction du modèle structurel adopté par l'organisation[3].

**Les structures en réseau**




Trois différents types de nœuds réseautiques sont présents au cœur des modèles présentés par Arquilla et Ronfeldt (2004) :

1. *Les nœuds critiques* : représentent les *têtes* des groupes terroristes. C'est à ce niveau que les décisions les plus importantes du groupe sont prises. Ces nœuds ne sont pas nécessaires au bon fonctionnement de l'organisation terroriste, mais ils contribuent à pousser le groupe dans des démarches innovatrices, tout en le conduisant à suivre des objectifs clairs et communs.
2. *Les nœuds névralgiques* : ce palier hiérarchique fait référence aux *cadres* des réseaux terroristes. Ils ont pour principale fonction de transposer les idées provenant du haut de l'organisation en gestes pragmatiques[4]. Ainsi, ce sont les cadres qui veillent à la mise sur pied des actions terroristes au quotidien (attentats, recrutement, entraî-

3 Une typologie similaire amenée par Jacques Beaud discute de l'importance des nœuds réseautiques au sein des organisations terroristes (Baud, 2003 : 55).

4 Cette fonction est d'autant plus importante dans les groupes terroristes religieux. En effet, dans ce genre de groupe, les cadres doivent pouvoir appliquer une idéologie religieuse, voire obscurantiste, à travers des actions terroristes concrètes. Ils doivent donc relever le difficile défi de faire cadrer la parole avec l'action, et ce, dans le but de donner une cohérence discursive au groupe terroriste. Le meilleur exemple de cela se trouve dans la relation qu'a Abu Musab Al Zarkawi avec Oussama ben Laden. Même si les deux personnages sont reliés au même réseau terroriste, en l'occurrence Al-Qaïda, ben Laden demeure un idéologue, alors que Zarkawi ne fait que transposer le discours du Jihad global en des actions concrètes sur le terrain, notamment en Irak (BBC News, 2005).

nement, acquisition de matériel, etc.) tout en s'assurant que les actions du groupe cadrent avec les volontés des têtes dirigeantes.

3. *Les nœuds opérationnels*: correspondent aux *soldats* des organisations terroristes. C'est à ce palier hiérarchique que se trouvent les individus qui commettent les attentats. Étant plus susceptibles de se faire arrêter par les autorités, ces membres de l'organisation terroriste ont habituellement moins de responsabilités et savent peu de choses des objectifs stratégiques du groupe.

Depuis la fin de la guerre froide, ce sont les structures réseautiques franchisées qui sont les modèles les plus fréquemment adoptés par les organisations terroristes. Elles ont l'avantage de fournir à l'organisation une direction à la fois assez souple et efficace du point de vue des communications. Toutefois, les faiblesses de ce modèle résident dans le fait que certains points du réseau demeurent fragiles aux opérations de sécurité. En effet, malgré une décentralisation assez évidente des activités, le réseau peut se faire décapiter assez aisément si les agences policières réussissent à frapper les nœuds critiques ou névralgiques.

C'est d'ailleurs pour répondre à cette faiblesse structurelle que certaines organisations terroristes tendent de plus en plus à se tourner vers les réseaux à matrice complexe[5]. Les structures organisationnelles à matrice complexe sont principalement issues des principes de la loi de Metcalfe qui stipule que la force, ou la valeur, d'un réseau est proportionnelle au carré du nombre de ceux qui l'utilisent (Gilder, 1993). L'exemple le plus typique de la force d'un réseau est celui du téléphone. Si seulement deux personnes utilisent le téléphone, cet outil n'est pas très utile. Toutefois, si chaque individu de la planète est muni d'un téléphone, alors cet instrument représente un atout indéniable pour une communication efficace. En d'autres termes, plus un réseau a de nœuds, et que ces nœuds se trouvent interconnectés les uns aux autres, plus ce réseau sera puissant.

Sur le plan social, la loi de Metcalfe signifie que l'interaction de plusieurs individus vers un objectif commun, le tout supposant une multi-

---

5 Les réseaux terroristes islamistes sont d'ailleurs reconnus pour privilégier ce genre de configuration hiérarchique. Cela entre dans la mentalité de la Oumma (Umma) qui fait référence à l'ensemble de la communauté des musulmans, et ce, au delà de leur nationalité et des pouvoirs politiques qui les gouvernent. Le principe de hiérarchisation est donc très différent de celui que nous pouvons distinguer au sein des organisations terroristes occidentales. En effet, le pouvoir politique est considéré comme accessoire au sein des organisations islamistes radicales, puisque tous les humains sont subordonnés à Allah. (Voir entre autres : Makrerougrass, 2003 et Rougier, 2004).

plicité de liens connexes entre tous les membres de l'organisation, décuplera leur capacité d'action. Par exemple, des terroristes travaillant pour la même organisation, mais œuvrant de manière isolée, peuvent certes être efficaces, mais ils le seront beaucoup plus s'ils collaborent à la réalisation de leurs objectifs communs. De là l'utilité de la loi de Metcalfe dans la théorisation structurelle des organisations terroristes.

De plus, comme le démontre le graphique 1, les réseaux à matrice complexe ont l'avantage de ne pas avoir de points faibles évidents.

> *Unlike a hierarchical network that can be eliminated through decapitation of its leadership, a small-world network (*réseau à matrice complexe*) resists fragmentation because of its dense interconnectivity. A significant fraction of nodes can be randomly removed without much impact on its integrity* (Sageman, 2004 : 140).

Cette structure complètement décentralisée, sans tête (*leaderless*), ne comporte pas de nœud critique et névralgique, reléguant ainsi les postes décisionnels à tous les nœuds du réseau. « *The strength of this form of organization is that all cells are independent of one another and the discovery of one cannot lead to the discovery of another* » (McAllister, 2004 : 302). Étant donné l'absence de lien hiérarchique entre les différentes cellules, le réseau est très difficile à faire tomber.

Or, non seulement un réseau à matrice complexe ne peut pas être décapité, mais en plus la perte d'une cellule du réseau n'a que très peu d'effet sur l'ensemble des activités terroristes. « *Having no "hub" to answer to, authority in an all-channel network* (réseau à matrice complexe) *is entirely decentralized, minimizing the impact of the destruction of individual cells on the organization as a whole* » (McAllister, 2004 : 302).

Cette structure sans tête se lie également à la notion de *réseau-stupide* formulée par David Isenberg (1998). Ses travaux sur les réseaux téléphoniques démontrent que dans un contexte d'incertitude, un réseau ne devrait jamais être optimisé pour accomplir une action précise. Il devrait plutôt adopter une structure simple (stupide) et polyvalente, et ce, pour demeurer efficace dans un large éventail de situations.

En transposant ces principes aux hiérarchies terroristes, le réseau terroriste doit donc s'assurer que les cellules qui le composent sont aptes à se mouler aux diverses situations qui peuvent se produire. L'objectif à atteindre est que chacune des cellules de l'organisation puisse accomplir toutes les tâches nécessaires pour perpétuer la cause : du financement du réseau jusqu'à l'accomplissement de l'attentat en passant par le recrutement et l'entraînement.

## 2. La tactique réseaucentrique comme modèle opérationnel

L'avantage le plus important de la structure hiérarchique à matrice complexe est la capacité de perpétrer des opérations dites réseaucentriques. Le terme d'opérations *réseaucentriques* provient du jargon militaire et est fortement lié au mouvement d'intégration des technologies de l'information dans les structures militaires, mieux connu sous le terme de *révolution dans les affaires militaires* (RAM) (Sloan, 2003). Dans leur article sur les opérations réseaucentriques, les auteurs Wesensten, Belenky et Balkin décrivent le concept ainsi :

> *Network-centric operations* [...] *are characterized by information-sharing across multiple levels of traditional echelons of command and control. This information-sharing is made possible by networking the entire force down to the individual level. Therefore, network-centric operations depend upon the availability of information on the status and disposition of friendly forces, enemy forces, and all other relevant aspects of the operational environment* [...] *An underlying assumption of information-sharing is that the latter translates into a shared situational awareness and self-synchronization through shared mental models of the current situation and of the desired end-state (synonymous with commander's intent, i.e., the object of the operation), leading to a war-fighting advantage* (Wesensten *et al.*, 2005 : 94-95).

Pour faire une analogie rapide, les opérations terroristes réseaucentriques sont au terrorisme ce que le commerce électronique est au monde des affaires.

En fait, comme le soulignent Albert et Hayes dans leur ouvrage *Power to the Edge : Command and Control in the Information Age*, le concept d'opération réseaucentrique :

> [...] *provides the theory for warfare in the Information age.* [...] *As such we can look to its tenets to see what is different about the information assumed to be available, how it is distributed and used, and how individuals and entities relate to one another. In other words, we can identify what is different about command and control* (Albert et Hayes, 2004 : 98).

Les opérations réseaucentriques entrent donc en droite ligne avec ce phénomène de redéfinition du militaire à l'âge des technologies de l'information.

À la lumière de cette description, on peut concevoir un cadre descriptif des opérations terroristes réseaucentriques. En faisant le lien avec le portrait des opérations réseaucentriques fait par Albert et Hayes (2004), nous pouvons affirmer que les opérations terroristes réseaucentriques permettent d'exploiter au maximum l'information, dans le but

d'améliorer les capacités de commandement et de contrôle des actions du groupe terroriste.

### *De nouvelles tactiques*

Les opérations réseaucentriques augmenteraient donc l'efficacité d'une structure à matrice complexe en lui permettant de contrôler efficacement et rapidement les différents nœuds réseautiques faisant partie de l'ensemble du réseau. En d'autres termes, il est désormais possible de faire bouger l'ensemble du réseau vers un objectif commun très rapidement en déployant très peu d'efforts de communication. En saisissant le plein potentiel des technologies de l'information et des communications modernes, un groupe terroriste peut désormais contrôler l'ensemble de ses activités en temps quasi réel, le rendant d'autant plus dangereux.

Une analyse des possibilités des opérations réseaucentriques nous amène à dire que ces dernières offrent trois nouvelles tactiques aux groupes terroristes. La première est la *tactique de la nuée*. Cette posture ultra-offensive consiste à donner l'ordre à tous les nœuds du réseau de perpétrer des attentats. Il s'agit donc de relâcher l'ensemble de la puissance du réseau terroriste dans toutes les directions en coordonnant une série d'attaques meurtrières.

Si, à première vue, cette tactique peut sembler impensable, puisqu'elle mettrait en danger bon nombre des éléments de l'organisation, elle correspond parfaitement à la mentalité des terroristes contemporains. Si les terroristes classiques semblaient chercher à limiter l'utilisation de la violence[6], aujourd'hui cette règle est caduque et on cherche plutôt à augmenter la létalité des actions :

> *The replacement of the coercive diplomacy model has been noted by some analysts who suggest that some groups have adopted a "war paradigm", where the strategic aim is to inflict damage generally and conventional constraints, resulting in proportionality, are not present. In such cases the instrumental use of violence gives way to a more "hostile" use of violence. It appears that religious groups would fit into this paradigm of motivation. The tendency of religious groups to perceive the conflict as a zero-sum game where no compromise is possible and as a battle between good and evil reinforces this perception of total war. This factor is also reinforced by the common tendency for religious groups to perceive their struggle in defensive terms. In a defensive struggle even violent actions which*

6 C'est, entre autres, la pensée de Bruce Hoffman (1998 : 197) qui stipule que les groupes terroristes classiques employaient la violence avec parcimonie et de manière sélective.

> *normally would not be legitimate can be justified as being reactive in character and therefore perceived as a legitimate means of self-defence. Thus the perception of religious groups that they are engaged in a total war and a defensive struggle reinforces and justifies the use of heightened levels of violence* (Ellis, 2003 : 5).

Ainsi, dans une telle vision des choses, la tactique de la nuée est tout à fait envisageable. Par exemple, elle peut s'avérer une *tactique de la dernière chance*, efficace dans l'éventualité où le groupe terroriste est mis en danger.

La seconde option est ce que nous appelons la *tactique de l'oursin*. Cette tactique, pouvant être caractérisée d'offensive-défensive, permet de coordonner différents éléments du réseau pour lancer plusieurs attaques. À l'image de l'oursin qui déploie des dards pour se défendre et repousser son adversaire, le groupe terroriste perpètre synchroniquement une série d'attentats à travers diverses cellules de l'organisation. Il s'agit donc de déployer le potentiel de quelques cellules, les faisant passer à un mode offensif. Cela a pour résultat de détourner l'attention des agences policières vers les cellules actives, augmentant ainsi la défense du reste du réseau. En suivant la métaphore de l'oursin, ce qui signifie de sacrifier quelques dards pour mieux protéger le corps.

La troisième option constitue l'option défensive par excellence et est donc à l'opposé de la tactique de la nuée. Il s'agit de la *tactique de l'éclatement*. Elle consiste à faire éclater l'organisation terroriste. Profitant de la grande indépendance des nœuds d'un réseau à matrice complexe, il s'agit de briser les liens entretenus entre les différentes cellules de l'organisation et de les laisser agir en complète autonomie. Elles peuvent donc se réorganiser de leur côté, redémarrer des réseaux parallèles, voire même perpétrer des attentats sans avoir à communiquer avec le reste du réseau. Adoptant cette tactique, la structure terroriste devient très difficile à comprendre pour les autorités qui doivent tenter de saisir la nouvelle structure organisationnelle d'une multitude de cellules.

Évidemment, il ne s'agit ici que d'un simple aperçu des possibilités offertes par les opérations réseaucentriques. En aucun cas nous n'affirmons que cela représente une liste exhaustive des avantages inhérents aux réseaux terroristes adoptant ce genre de fonctionnement organisationnel. En effet, d'autres possibilités s'ajoutent aux opérations réseaucentriques.

Par exemple, dans leur texte sur les structures réseaucentriques, Zanini et Edwards (2001 : 31-32) mentionnent trois autres avantages liés à ce type d'opérations :

> *First, communication and coordination are not formally specified by horizontal and vertical reporting relationships, but rather emerge and change according to the task at hand.* [...] *Second, internal networks are usually complemented by linkages to individuals outside the organization, often spanning national boundaries.* [...] *Third, both internal and external ties are enabled not by bureaucratic fiat, but rather by shared norms and values as by reciprocal trust.*

Les deux premiers aspects mentionnés par les auteurs soulignent le fait que les opérations réseaucentriques complexifient davantage les relations entre les membres d'une organisation terroriste. Les liens ne sont donc plus clairement définis entre les cellules et vont souvent s'inscrire dans des relations avec des groupes terroristes satellites.

Le troisième aspect, lui, est on ne peut plus important, car il fait référence aux caractéristiques psychologiques nécessaires au bon fonctionnement des opérations réseaucentriques. L'application des principes réseaucentriques au contexte du terrorisme affecte directement la dynamique de groupe. Les individus présents au sein des organisations terroristes finissent par adopter une vision particulière de la réalité. En effet, la dynamique groupale fait en sorte que plus un individu construit son identité par une vision partagée au sein d'un groupe, moins il est capable d'anticiper les idées se trouvant à l'extérieur du groupe (Combs, 2003 : 62). Or les réseaux sociaux sont décrits comme étant des : « [...] *complex communicative networks that create shared worlds of meaning and feelings, which in turn shape identity, perception, and preferences* » (Sageman, 2004 : 158). Le constat qu'il faut donc faire est que les opérations réseaucentriques se nourrissent de la dynamique de groupe (du sens idéologique commun) tout en permettant d'entretenir cette même dynamique en structurant la pensée des individus vers des modes de fonctionnement collectifs fermés sur eux-mêmes. En d'autres termes, le réseau social devient le seul point de référence sociopsychologique et conditionne la psyché des terroristes vers des objectifs qui ne servent qu'au groupe.

### *La dépendance des opérations réseaucentriques aux technologies de l'information*

Il faut tout de même mentionner que l'aspect le plus important des opérations terroristes réseaucentriques est l'exigence d'exploiter systématiquement les technologies de l'information. Le fait étant que, pour être apte à commander et contrôler à distance différentes cellules terroristes se trouvant un peu partout sur la planète, et ce, de manière synchronique, les opérations réseaucentriques doivent être coordonnées, néces-

sitant un système de communication efficace. Les opérations réseaucentriques sous-tendent nécessairement un emploi systématique des technologies de l'information et des communications dans le cadre de la gestion des activités du groupe terroriste. C'est d'ailleurs pour cette raison que nous assistons de plus en plus à la montée de ce que nous pouvons nommer la cyberplanification (Thomas, 2003 : 117), l'utilisation des technologies de l'information, principalement l'Internet, mais aussi la téléphonie cellulaire et les messageries texte instantanées, pour gérer les activités d'un groupe. Cette tendance est de plus en plus présente chez les groupes terroristes, notamment chez Al-Qaïda :

> *During the Sudanese exile, rapid changes in communication technology spread around the world. The global Salafi jihad was quick to grasp its possibilities. Osama bin Laden brought a new satellite telephone during that time. Al Qaeda operatives started to use laptop computers to store information and send e-mail to each other. Fax transmission was used to release communiqués in London sent from undisclosed sites. Dedicated web sites informed mujahedin and their supporters of new developments in the jihad.* [...] *This new technology enabled a global jihad based on a loose, decentralized network of mujahedin transcending the limitations of face-to-face interaction* (Sageman, 2004 : 159).

En fusionnant les possibilités offertes par les technologies de l'information avec ses pratiques, Al-Qaïda a réussi à se forger un réseau capable de perpétrer les attentats du 11 septembre 2001 et résister à plus de trois ans de lutte contre le terrorisme. Aujourd'hui, l'utilisation des technologies de l'information par ce groupe terroriste est encore plus prépondérante. Par exemple, en exploitant le potentiel des technologies de l'information, le groupe a réussi à fomenter l'attentat de Madrid sans réunion physique de ses membres[7]. En fait, depuis l'invasion étatsunienne en Afghanistan, Al-Qaïda s'est presque complètement tournée vers la cyberplanification (Anderson, 2004).

Certes, ce type d'organisation électronique permet une gestion appropriée des opérations réseaucentriques, mais cela a aussi l'avantage d'éviter les déplacements des membres du groupe, leur évitant de se faire repérer par les autorités chargées de la sécurité. Bref, sans ces technologies et les communications efficaces et relativement anonymes qu'elles permettent, les groupes terroristes seraient obligés de s'en remettre à une structure organisationnelle plus archaïque, comme les hiérarchies pyramidales ou les réseaux franchisés, par exemple. Conséquemment,

---

7 Selon les différentes enquêtes menées, l'attentat aurait été planifié sur le Web, plus précisément sur des forums de discussions (Frantz *et al.*, 2004).

cela risquerait de mettre en danger la survie même de leurs organisations, car elles deviendraient plus vulnérables aux opérations policières.

### *Les attentats de Londres : un exemple d'opération terroriste réseaucentrique*

L'attentat terroriste du 7 juillet 2005 à Londres est l'exemple le plus probant d'attaque terroriste basée sur les principes des opérations réseaucentriques. L'enquête menée à la suite de l'attaque a démontré qu'elle avait été perpétrée par un groupe d'individus qui n'étaient pas directement reliés à la nébuleuse d'Al-Qaïda. Certes, ils entretenaient des relations avec certains membres suspectés d'appartenir au mouvement, mais il n'y avait pas de planification hiérarchisée de l'opération ; les ordres n'allaient pas du haut vers le bas.

Les *chaînes de commandement* sont donc essentiellement fondées sur des relations interpersonnelles complexes, forgées par l'entremise de rencontres informelles (Roy, 2004 : 25). Cette *informalité* présente dans l'opération se répercute d'ailleurs dans la revendication de l'attentat de Londres. L'attaque a été à la fois revendiquée par l'organisation Al-Qaïda-Jihad en Europe et deux jours plus tard par les Brigades Abou Hafs al-Masri, division d'Europe[8] (Mahjoub, 2005).

De plus, le mode opérationnel des attentats de Londres peut s'apparenter, en substance du moins, à la tactique réseaucentrique de la nuée. Les auteurs de l'attentat se connaissaient tous et n'étaient pas directement liés — en apparence du moins — à des mégastructures terroristes, et ont tous passé à l'action en même temps (Reuters/AFP, 2005). Cette unicité dans l'attentat a non seulement permis la commission d'un acte efficace, mais a également protégé le reste du réseau terroriste : les terroristes impliqués dans l'acte se sont suicidés et ont emporté ce qu'ils savaient avec eux.

Cela confirme donc le mode de fonctionnement des terroristes contemporains. Ils organisent leurs relations et la préparation de leurs opérations selon les principes des théories réseaucentriques. Une fois l'attaque commise, l'attentat est revendiqué par un *label* ; une organisation

8 Ce second groupe est le même qui avait revendiqué les attaques de Madrid du 11 mars 2004. En fait, ils ont revendiqué bon nombre d'attentats à travers le monde (Janabi, 2004). Le groupe semble toutefois de moins en moins crédible, surtout depuis qu'il a revendiqué les coupures d'électricité au Canada et aux États-Unis à l'été 2003 (Raizon, 2005).

phare qui peut aisément soutenir idéologiquement la cause. Dans le cas de Londres, Al-Qaïda fut le substrat idéologique.

## 3. Les faiblesses des opérations terroristes réseaucentriques

Nous l'avons déjà mentionné, les groupes terroristes adoptant un mode de fonctionnement réseaucentrique représentent des défis importants pour ceux qui décident des stratégies de sécurité.

> *Assessing the impact of counter-terrorism operations against such actors is also more difficult due to the fact that only portions of the network may be identified and targeted, while other parts of the network remain unknown and viable in the face of such operations. In particular, counter-leadership strikes would be less effective against decentralized actors lacking centralized command and control procedures. Actors with such decentralized structures are more flexible and better able to adapt to changed circumstances* (Ellis, 2003 : 13).

En d'autres termes, ce type d'opérations permet aux organisations terroristes d'être plus efficaces et leur permettent de mieux résister à un environnement hostile.

Quand on considère les structures terroristes réseaucentriques, il faut garder à l'esprit qu'elles sont le résultat de décisions prises par le groupe. C'est donc l'organisation terroriste elle-même qui décide d'agencer ses activités selon ses propres besoins. Évidemment, la décision de transformer les activités du groupe est conditionnée par l'environnement dans lequel les terroristes évoluent. Cela signifie que les structures terroristes ne sont pas des éléments figés. Le meilleur exemple de cette malléabilité structurelle se trouve dans le modèle hiérarchique adopté par Al-Qaïda au lendemain de l'invasion en Afghanistan. Pour faire face à la machine états-unienne chargée de la sécurité, l'organisation a dû employer la tactique de l'éclatement et se réorganiser autrement (Jenkins, 2002 : 10). Une analyse d'ailleurs partagée par Gunaratna dans ses travaux sur les capacités d'Al-Qaïda :

> Aujourd'hui, Al-Qaïda connaît une période de transition [...] Malgré le démantèlement de son infrastructure opérationnelle et de formation en Afghanistan, Al-Qaïda s'adapte en cherchant à établir ses bases ailleurs et, de ce fait, demeure une menace sérieuse, immédiate et directe pour ses ennemis. Bien que partout dans le monde, l'infrastructure matérielle et humaine d'Al-Qaïda ait souffert, son réseau à travers le monde, constitué de multiples strates, a conservé une profondeur suffisante pour planifier, préparer et exécuter des opérations, soit directement, soit par

> le truchement des groupes qui lui sont associés (Gunaratna dans Chaliand et Blin, 2004 : 465).

Ce constat indique que les organisations terroristes réagissent, d'une manière quasi biologique, à l'environnement dans lequel elles évoluent. Cette réactivité peut, à terme, être exploitée par les autorités chargées de la sécurité afin d'affaiblir les réseaux terroristes. Il s'agirait, par exemple, de forcer les terroristes à abandonner les opérations réseaucentriques et à passer d'une structure à matrice complexe vers un mode hiérarchique plus classique, comme les réseaux franchisés. Les réseaux terroristes deviendraient donc plus fragiles face aux opérations de sécurité, notamment les opérations de décapitation.

Pour y arriver, il faut que les terroristes perçoivent que l'organisation est en danger. Les travaux d'Albert et Hayes (2004 : 32) sur les opérations réseaucentriques militaires démontrent que : « [...] *in order to work together effectively in this mode, the elements of this force will have to achieve a high level of trust. At a minimum, this means that they must have exercised together successfully across the range of missions involved* ». Il est fort probable que la même situation se retrouve au sein des opérations réseaucentriques terroristes ; les différents nœuds des réseaux à matrice complexe sont nécessairement unis par de forts liens de confiance. Ce sont ces liens de confiance qui, lorsque brisés, engendrent des transformations dans la structure terroriste.

Les membres des organisations terroristes qui perçoivent des bris de confiance dans leurs relations vont nécessairement s'inquiéter et repenser leur mode de fonctionnement. Selon la gravité de cette fracture et des décisions prises par les *têtes pensantes* de l'organisation, il est probable qu'une recentralisation des activités soit opérée. Cette recentralisation serait effectuée dans l'optique d'acquérir un contrôle sur les liens relationnels entre les cellules. C'est cette recentralisation qui comporte un risque pour les groupes terroristes, puisqu'elle restructure les activités en fonction de hiérarchies plus dirigistes, où plusieurs cellules deviennent dépendantes d'une cellule en position d'autorité pour fonctionner. Se dessine alors une structure plus fragile face aux opérations de sécurité cherchant à frapper les têtes du réseau.

Première façon de briser la confiance des réseaux à matrice complexe qui exploitent les opérations réseaucentriques : utiliser leur dépendance envers les technologies de l'information. Cette manière de faire est d'ailleurs bien exprimée par Brent Ellis :

> *While networked structures offer advantages* [...] *they also have weaknesses. The adoption of a networked structure increases the level of communications necessary for the network to operate, and thus, decreased control over the management of such communications. Both the number of transmissions and the range of formats utilized may have to be increased. This may increase the potential for surveillance and intelligence gathering opportunities. If the adoption of networked structures is related to the revolution of information technology* [...] *the increased use of information technology by networked terrorist may also increase their vulnerability to signals intelligence penetration* (Ellis, 2003 : 14).

Ainsi la dépendance des opérations réseaucentriques envers les technologies de l'information est une faiblesse intrinsèque à ce mode de fonctionnement. En étant obligés d'utiliser ces technologies, les groupes terroristes se rendent plus vulnérables à des opérations de renseignement électronique ou ELINT (*electronic intelligence*) et de renseignement signalétique ou SIGINT (*signals intelligence*) [Federation of American Scientist, 1997].

Il est aussi clair que des opérations de renseignement plus classiques, comme le renseignement humain ou HUMINT (*human intelligence*), par exemple, représentent des solutions envisageables pour déstabiliser les réseaux terroristes. En effet, l'infiltration des réseaux terroristes peut devenir un excellent moyen de briser les liens de confiance entre les cellules, et ce, de l'intérieur même des organisations. Néanmoins, ces opérations demeurent très difficiles à mettre sur pied et sont grandement risquées pour les agents de renseignement, surtout dans le cadre d'organisations terroristes employant la tactique du terrorisme suicidaire.

La dernière méthode, prônée par les États-Unis, pouvant servir à briser la confiance au sein d'un réseau terroriste exploitant les opérations réseaucentriques, est l'utilisation des opérations psychologiques. Les opérations psychologiques se fondent sur des techniques diverses de manipulation de l'information, afin de poursuivre et d'atteindre des objectifs militaires ou politiques auprès de certaines cibles, qui comprennent notamment : la volonté nationale ennemie ou amie ; le commandement ennemi ; les troupes ennemies ou amies ; la société ennemie ou amie (Joint Chiefs of Staff, 1996).

Les opérations psychologiques consistent donc, entre autres, à disséminer ou manipuler des informations qui seraient susceptibles de transformer la perception qu'a l'adversaire de son environnement. Ainsi, en se basant sur les principes des opérations psychologiques, combattre les opérations réseaucentriques consisterait à faire en sorte que les terroristes croient que les liens de confiance entre les différentes cellules du

réseau sont corrompus. Cela forcerait l'organisation à restructurer ses activités, et possiblement centraliser le processus décisionnel. Encore une fois, par le démantèlement du fonctionnement en réseau, l'organisation deviendrait plus vulnérable à des opérations de *décapitation*.

## Conclusion

Comme nous avons pu le voir au cours de ce texte, les organisations terroristes tendent de plus en plus à adopter des structures organisationnelles en réseaux décentralisés que nous appelons des réseaux à matrice complexe. Ces nouveaux modes d'organisation permettent aux terroristes de mieux s'adapter à l'environnement de sécurité actuel. Cela leur donne aussi l'occasion de se doter de nouvelles options opérationnelles par les opérations réseaucentriques. Il y a toutefois un prix à payer pour exploiter les possibilités offertes par ces nouvelles structures hiérarchiques. En effet, étant donné qu'elles demandent un haut degré de coordination, les opérations réseaucentriques nécessitent l'emploi systématique des moyens de communication issus des technologies de l'information. Conséquemment, cela place les groupes terroristes en position de dépendance face à ces technologies, ce qui, à terme, pourrait représenter un risque important pour la sécurité même de leurs organisations. La plus importante vulnérabilité des réseaux est probablement le nécessaire lien de confiance qui doit exister en permanence entre les différentes cellules d'un groupe terroriste. Cette faille structurelle représente donc une occasion intéressante pour les agences policières.

D'un point de vue analytique et théorique, il ressort clairement que les organisations terroristes ne doivent pas être étudiées comme étant des mouvements statiques. Comme il a été possible de le constater, les groupes terroristes répondent à des dynamiques internes et externes. D'un côté, les réseaux terroristes s'organisent en fonction de leurs propres objectifs et leur vision du monde. De l'autre côté, ces groupes doivent également s'adapter à l'environnement dans lequel ils sont appelés à évoluer. De ce fait, cette dynamique pousse les terroristes à user d'innovation dans leurs structures organisationnelles, et ce, pour devenir plus efficaces face aux autorités chargées de la sécurité.

## Références


Albert, D. S. & Hayes, R. E. (2004). *Power to the Edge : Command and Control in the Information Age.* Washington DC : Command and Control Research Program Publication Series.

Anderson, K. (2004). *Militants weave web of terror.* Consulté le 24 février 2006, http://news.bbc.co.uk/2/hi/technology/3889841.stm.

Arquikka, J. & Ronfeldt, D. (2001). *Networks and Netwars : The Future of Terror, Crime, and Militancy.* Santa Monica : National Defence Institute RAND.

Baud, J. (2003). *La guerre asymétrique ou la défaite du vainqueur.* Paris : Du Rocher.

BBC NEWS (2005). *Profile : Abu Musab al-Zarqawi.* Consulté le 24 février 2006, http://news.bbc.co.uk/2/hi/middle_east/3483089.stm.

Berman, P. (2003). *Terror and Liberalism.* New York : W. W. Norton & Company.

Chaliand, G. & Blin, A. (dir.) (2004). *Histoire du terrorisme : de l'Antiquité à Al-Qaïda.* Paris : Bayard.

Combs, C. C. (2003). *Terrorism in the Twenty-First Century.* Upper Saddle River : Prentice Hall.

Ellis, B. (2003). Countering Complexity : An Analytical Framework to Guide Counter-Terrorism Policy-Making. *Journal of Military and Strategic Studies, 6* (1), 1-20.

Federation of American Scientist (1997). *SIGINT Overview.* Consulté le 24 février 2006, http://www.fas.org/spp/military/program/sigint/overview.htm.

Frantz, D., Meyer, J. & Schmitt, R. B. (2004). *Cyberspace Gives Al Qaeda Refuge.* Consulté le 24 février 2006, http://www.jihadwatch.org/archives/002871.php.

George, A. (1991). *Western State Terrorism.* New York : Routledge.

Gilder, G. (1993). *Metcalfe's Law and Legacy.* Consulté le 24 février 2006. http://www.discovery.org/scripts/viewDB/index.php?command=view&program=Technology and Democracy - Innovation&id=41.

Hoffman, B. (1999). *Inside Terrorism.* New York : Columbia University Press.

Isenberg, D. (1998). *The Dawn of the Stupid Network.* Consulté le 24 février 2006. http://www.isen.com/papers/Dawnstupid.html.

Janabi, A. (2004). *Profile : Abu Hafs al-Masri.* Consulté le 24 février 2006, http://english.aljazeera.net/NR/exeres/D2D48F79-B330-40E3-A17D-B4CDD01EE1A0.htm.

Jenkins, B. M. (2002). *Countering Al Qaeda : An Appreciation of the Situation and Suggestions for Strategy.* Santa Monica : National Defence Institute RAND.

Joint Chiefs of Staff (1996). *Doctrine for Joint Psychological Operations.* Consulté le 24 février 2006, http://www.iwar.org.uk/psyops/resources/us/jp3_53.pdf.

Laqueur, W. (2000). *The New Terrorism : Fanaticism and the Arms of Mass Destruction.* New York : Oxford University Press.

Lesser, I. O., Hoffman, B., Arquilla, J., Ronfeldt, D. & Zanini, M. (1999). *Countering the New Terrorism*. Santa Monica : RAND Corporation.

Mahjoub, T. (2005). Al-Qaeda lance un ultimatum à l'Europe. *Cyberpresse*. Consulté le 10 septembre 2005. http://www.cyberpresse.ca/monde/article/article_complet.php?path=/monde/article/19/1,151,1064,072005,1106046.php.

Makrerougrass, A. (2003). *L'État islamique, dernière des ignorances*. Québec : Presses Universitaires de Laval.

Mannoni, P. (2004). *Les logiques du terrorisme*. Paris : In press.

Martin, J. M. & Romano, A. T. (1992). *Multinational Crime : Terrorism, Espionage, Drugs & Arms Trafficking*. Newbury Park : Sage Publications.

McAllister, B. (2004). Al Qaeda and the Innovative Firm : Demythologizing the Network. *Studies in Conflict and Terrorism*, *27* (4), 297-319.

Morgan, M. J. (2004). The Origins of the New Terrorism. *Parameters*, *34* (1), 29-43.

Organisation des Nations Unies (1999). *Convention internationale pour la répression du financement terroriste*. Consulté le 24 février 2006, http://untreaty.un.org/French/Terrorism/Conv12.pdf.

Raizon, D. (2005). *Al-Qaïda lance un ultimatum à l'Europe*. Consulté le 24 février 2006, http://rfi.fr/actufr/articles/067/article_37609.asp.

Reuters/AFP (2005). Attentats de Londres — Une enquête de plus en plus internationale. *Le Devoir*. Consulté le 10 septembre 2005. http://www.ledevoir.com/cgi-bin/imprimer?path=/2005/07/28/86378.html.

Rougier, B. (2004). *Le Jihad au quotidien*. Paris : Presses universitaires de France.

Roy, O. (2004 : septembre). Al-Qaïda, label ou organisation ? *Le monde diplomatique*. Consulté le 24 février 2006, http://www.monde-diplomatique.fr/2004/09/ROY/11440.

Rubin, B. & Rubin, J. C. (2002). *Anti-American Terrorism and the Middle East*. New York : Oxford University Press.

Sageman, M. (2004). *Understanding Terror Networks*. Philadelphia : University of Pennsylvania.

Sloan, E. C. (2003). *The revolution in military affairs : Implications for Canada and NATO*. Montréal : McGill-Queens University Press.

Thomas, T. L. (2003). Al Qaeda and the Internet : The Danger of "Cyberplanning". *Parameters*, *33* (1), 112-123.

Tucker, D. (2001). What is New about the New Terrorism and How Dangerous is it ? *Terrorism and Political Violence*, *13* (3), 1-14.

Wesensten, N. J., Belenky, G & Balkin, T. J. (2005). Cognitive Readiness in Network-Centric Operations. *Parameters*, *35* (1), 94-105.