Dr. Kerti András: **Cyberterrorisme**

L'absence de débats publics dans les régimes autocratiques ou son insuffisance dans les régimes démocratiques, ont permis de donner encore plus de relief à l'émergence d'un nouveau média, internet, qui non seulement dispense des informations non institutionnelles, mais facilite également la connexion des opinions publiques entre elles. Cette mondialisation de l'accès à l'information s'est également accompagnée d'une tentative de récupération de cette fenêtre de communication par les franges les plus radicales de nos sociétés. En effet, si internet a facilité les échanges et rapproché les civilisations, il a donné également la possibilité aux mouvements terroristes de profiter d'un certain nombre d'opportunités technologiques avec ce que cela comporte en terme de réduction des distances, de simplification des processus de décision et d'imagination du mode opératoire des attentats et d'impact sur les médias ainsi que sur les opinions. Le basculement dans le terrorisme islamiste mondial se fait à partir du moment où internet prouve son efficacité, c'est-à-dire la seconde moitié des années 1990. Ce n'est donc pas un hasard si de plus en plus de rapports et d'analyses révèlent la présence d'un nombre croissant d'informaticiens et d'ingénieurs au sein de la mouvance djihadiste. Plus inquiétant, l'accès aux informations comprend un volet très dangereux avec la recherche de données en matière d'armes de destruction massive. Des terroristes arrêtés en Grande-Bretagne et en Italie ont reconnu lors de l'enquête leur intérêt pour la possession de substances chimiques, bactériologiques ou nucléaires. Après avoir montré comment les terroristes, essentiellement djihadistes, utilisent internet comme vecteur de puissance, il conviendra d'analyser quelles sont les réponses apportées par les Etats pour lutter contre ce phénomène et de mettre en évidence les difficultés auxquelles ils restent confrontées.

Pour comprendre la stratégie des terroristes de récupération du web et en déduire qu'elle constitue un vecteur de puissance, il faut tout d'abord examiner sa logique fondée sur la déterritorialisation et la dématérialisation de ses acteurs pour ensuite s'arrêter sur les effets recherchés, à destination tant du monde musulman que des occidentaux.

Depuis la montée en puissance d'internet, le terrorisme a muté sur le fond comme dans la forme. Sur le fond, la toile a permis aux stratégies terroristes d'amplifier la dynamique de déterritorialisation de leur combat dans un monde de plus en plus globalisé. Dans la forme, le net a favorisé le développement de nouvelles techniques terroristes poussées par les phénomènes de dématérialisation que l'outil virtuel pouvait suggérer en matière de circulation des données, de prosélytisme et de communication entre terroristes. Internet crée des communautés qui peuvent ainsi s'émanciper de l'emprise d'un imam local et s'approprier l'islam par l'intermédiaire d'une autorité virtuelle devenue la nouvelle référence. L'incarnation des terroristes est de moins en moins importante au fur et à mesure qu'ils deviennent des icônes, que l'on peut consulter à tout moment sur le web. De plus, sur le réseau, le temps aussi est aboli et c'est ainsi que des textes médiévaux particulièrement guerriers seront reproduits sans aucune adaptation pour des auditoires qui n'ont pas forcément le recul pour les relativiser. Des injonctions dépassées, décontextualisées prennent grâce à internet, des accents de modernité. Ce phénomène se trouve amplifié par la mise en oeuvre sur le net du principe de l'irresponsabilité par la non-signature.

Internet permet donc aux terroristes de produire un effet de puissance de leur mouvement, de montrer qu'ils sont plus nombreux qu'on ne le pense. Il agit comme une caisse de résonance et donne visibilité et intelligibilité aux terroristes. Certains individus basculent ainsi progressivement de la sympathie pour des chefs insaisissables, véritables icônes du djihad, à l'action terroriste elle même. Les attentats sont calculés pour leur caractère audacieux et spectaculaire afin d'être sûr de créer un événement médiatique qui récolte un maximum d'audience. Il y a une pensée de la société du spectacle, à savoir que c'est avec la "mise en scène" de l'attentat que celui-ci prend sa

signification. Internet permet de véhiculer l'émotion par les images et l'idéologie par les textes et les discours. Le but étant de renverser les signes, les conventions : l'idéologue planétaire exposera en arabe la rationalité de l'action et l'exécutant s'exprimera dans le langage normalement universel, l'anglais. C'est notamment ce qui s'est produit lors de la revendication des attentats de Londres de juillet 2005.

Incontestablement, les attentats de New York, de Washington, de Madrid et de Londres ont changé la donne en matière de lutte contre le terrorisme. Mais au-delà des dispositions prises à l'ONU, aux Etats-Unis, ou dans l'UE, la question d'équilibrer le volet répressif et le respect des libertés individuelles n'a pas trouvé de solution consensuelle. En cela, l'internet met en exergue ce problème majeur. Les sites du djihad posent un dilemme aux services de renseignement. Les méthodes varient d'un pays et d'un contexte à l'autre. A Londres, pendant longtemps, la tactique suivie consistait à surveiller les sites djihadistes. Depuis les attentats des 7 et 21 juillet 2005, les policiers britanniques sont passés à l'action systématique de fermeture de ces supports du djihad. Les partisans du suivi du net estiment quant à eux que c'est en identifiant certains individus avec des écoutes téléphoniques et en remontant les réseaux, que l'on peut obtenir des résultats. C'est de cette manière qu'ont été identifiés et arrêtés les deux grands opérationnels des attentats du 11 septembre. De plus, afin notamment de traquer le djihadisme en ligne, un projet de loi contre le terrorisme a été présenté courant automne 2005 par le gouvernement et vient d'être adopté par l'Assemblée nationale. Il contient deux volets concernant internet : la surveillance des cybercafés et des fournisseurs d'accès.

C'est d'ailleurs l'enjeu de toutes les législations qui sont en train de se mettre en place. Les logs, les données internet des cybercafés, des fournisseurs d'accès, des hébergeurs seront légalement stockés pendant plusieurs mois, voire des années. L'intérêt est qu'en cas d'interpellation d'un présumé terroriste, les services de renseignement pourront remonter toutes les communications sur du long terme. Sur le web, la surveillance des réseaux est l'une des missions de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. La police du net repère les sites dont le contenu est sensible, surveille les forums où les propos tenus sont violents et trace les origines des sites internet impliqués. Viennent ensuite la localisation des auteurs et l'identification des visiteurs assidus des sites djihadistes. Pour ce faire, des logiciels permettent de remonter aux origines d'un serveur (localisation géographique d'un site) ou de tracer une adresse IP. Dans cette chasse aux contenus illégaux, des entreprises privées peuvent mettre à disposition leur expertise. Par exemple, la société Advestigo a mis au point un système qui permet de trouver sur la toile toute forme de contenu dès lors qu'il en possède une copie. Ce "renifleur" du web, conçu originellement pour traquer la contrefaçon numérique, peut être utilisé dans la lutte antiterroriste. En effet, il pourrait automatiser la recherche des sites publiant des manuels terroristes, ou les "recettes" pour réaliser une bombe.

Les services de renseignement américains ou européens et ceux dont les pays sont souvent visés par le terrorisme, se heurtent à des contraintes technologiques, politiques et judiciaires. Sur le plan technologique, l'usage du logiciel Skype permet à ses utilisateurs de communiquer sur la toile sans passer par un serveur susceptible d'être traqué par les services de sécurité. Selon les experts, les groupuscules extrémistes musulmans recourent aussi à la stéganographie adaptée à internet: les messages, ordres ou cartes passent via des photos anodines, des morceaux de musique MP3 et de la vidéo. Il existe également des experts en système de sécurité sur internet qui apportent leur concours à des groupes terroristes. L'un d'entre eux collabore avec les terroristes en mettant en ligne leurs vidéos et en protégeant leurs sources originales. Il est notamment entré dans un serveur STP de l'Etat pour y mettre des vidéos de décapitation.

Sur le plan judiciaire, la lutte contre le terrorisme relève encore de la compétence des Etats, alors que le terrorisme est un phénomène transnational. Certains pays dans lesquels les organisations islamistes radicales sont parfaitement légales laissent des sites publier des discours qui ne seraient

pas diffusables. Aux Etats-Unis, les sites révisionnistes sont tolérés, protégés par le premier amendement de la constitution. Il y a dans ce domaine encore trop de disparités alors qu'une harmonisation des législations s'impose. Sur le plan politique, partis, syndicats, organisations non gouvernementales et opinions publiques sont plus ou moins sensibles à la protection des libertés individuelles et à la cause défendue par les terroristes. Pour les spécialistes américain des questions de cyberterrorisme, le problème est triple. Outre les difficultés techniques, il pointe du doigt l'absence de coordination stratégique entre les services de renseignement occidentaux. Il souligne aussi le manque de savoir ou encore l'absence de formation des agents (langue et technologies) dans ce domaine. Une filière universitaire dédiée à la politique antiterroriste vient d'ailleurs d'être créée aux Etats-Unis, avec un séminaire consacré à la lutte contre le djihadisme en ligne. Dans le même registre, c'est bien souvent le personnel chargé de traiter la masse d'informations concernant ce phénomène qui est en nombre insuffisant. Or l'exploitation des données doit s'effectuer à chaud notamment dans le but de se prémunir efficacement contre la réalisation d'un attentat. Comme nous venons de le voir, l'utilisation par les réseaux terroristes du virtuel à des fins terroristes est bien une réalité. La lutte, bien engagée, contre ce nouveau vecteur du terrorisme doit pour gagner en performance et en efficience, se poursuivre en portant l'effort sur l'harmonisation et la formation. S'agissant de l'harmonisation, il est nécessaire d'aboutir à l'instauration d'une véritable législation internationale en matière de lutte contre le cyberterrorisme. Celle ci pourrait d'ailleurs s'inspirer de celle qui vient d'être adoptée en France. Il est primordial d'apporter une réponse unique et mondiale à un problème clairement transnational. Cette harmonisation passe également par une coopération renforcée au niveau international des services nationaux en charge des questions de terrorisme: échanges accrus de renseignements, actions communes, facilitation des investigations, autant de pistes qui méritent d'aboutir sur des initiatives concrètes. Sur le plan de la formation, l'effort doit porter tant sur l'approfondissement et l'actualisation des connaissances que sur des actions de sensibilisation. Les professionnels chargés de surveiller la toile ont en effet besoin d'étoffer en permanence leurs bases de données.

Références

[1] Rajnai Zoltán**:** Les radios de l'avenir pour les armées, In: Fekete Károly: Kommunikáció 2004., Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2004. pp. 269-273.

[2] Rajnai Zoltán-Sándor Miklós: Út a digitális kommunikációs rendszer felé (II.), NEMZETVÉDELMI EGYETEMI KÖZLEMÉNYEK (ISSN: 1417-7323) 1. évf.: (2. szám) pp. 217-229. (1997)

[3] Rajnai Zoltán-Fregan Beatrix: Un portrait militaire au reflet de l'insurrection hongroise ORIENTS (ISSN: 1769-6321) 2013: (10) pp. 93-96. (2013)