Le cyber-terrorisme. Le discours des médias américains et ses impacts

par Maura CONWAY

| Presses Universitaires de France | *Cités*

2009/3 - n° 39
ISSN 1299-5495 | ISBN 9782130572534 | pages 81 à 94

Le cyber-terrorisme. Le discours des médias américains et ses impacts

MAURA CONWAY

Après le 11 septembre 2001, un ressort essentiel des politiques américaines de renforcement de la « sécurité nationale » a pris la forme d'une insistance quasi paranoïaque sur les menaces potentiellement catastrophiques constituées par le cyber-terrorisme. Un grand nombre de commentateurs politiques, militaires ou économiques, ainsi que d'universitaires et de journalistes, ont envahi les plateaux de télévision ou ont été cités dans les journaux annonçant des attaques terroristes sur les infrastructures informatisées – ou par leur moyen. Structures auxquelles se rattachent de nos jours tous les aspects ordinaires de la vie urbaine aux États-Unis. Minutieusement décrits comme des infrastructures « hypercritiques », les systèmes informatiques sont apparus comme le talon d'Achille des sociétés industrielles avancées. Et avec d'autant plus d'insistance que, lors des attaques physiques de 2001, ce sont de banales infrastructures urbaines qui ont été effectivement utilisées comme armes autant que cibles pour provoquer les morts massives que l'on sait.

Dans les années 1990, c'était avec le débat plus global sur la protection des grandes infrastructures que les cyber-menaces avaient commencé à faire l'objet d'une attention accrue de la part du gouvernement fédéral américain. On s'était alors particulièrement préoccupé du fait que des ennemis des États-Unis incapables de vaincre les forces américaines sur les champs de bataille conventionnels pussent utiliser d'autres approches pour infliger des dégâts à l'unique superpuissance restante. Les événe-

Cités 39, Paris, PUF, 2009

ments du 11 septembre 2001 ont donc choqué de nombreux officiels du gouvernement américain, et même à un double titre : non seulement parce que les attaques ont été en elles-mêmes effroyables, mais aussi parce que leur nature conventionnelle (quoique asymétrique) était totalement inattendue. Or bien loin de diminuer la crainte d'une cyber-attaque, les attentats de 2001 ont eu pour effet d'accroître la crédibilité de la cyber-menace. La crainte du cyber-terrorisme était dans l'air du temps, et cet essai cherche à montrer l'émergence d'un « schème de la menace » qui plonge ses racines dans les événements d'alors.

L'argument principal de notre réflexion tourne autour de l'activité des médias américains, qui ont joué un rôle capital non seulement dans la propagation mais également dans l'élaboration proprement dite du schème toujours prévalant à ce jour de la menace cyber-terroriste. Si l'on va même un peu plus loin, c'est leur insistance sur la connexion fatale – quoique imaginaire – entre les réseaux virtuels et les infrastructures physiques qui a donné tant de force au concept de cyber-terrorisme.

FONDEMENTS THÉORIQUES : UNE POLITIQUE DE LA MENACE

Dans les études traditionnelles sur la sécurité, on estime que l'*imaginaire* de la menace ne fait pas vraiment problème et que ce sont les menaces *effectives* du monde réel qui se reflètent dans les politiques de sécurité. Mais on peut soutenir qu'il n'existe au contraire aucun lien naturel ni même évident entre la substance d'un « imaginaire de la menace » et la question de savoir s'il a un impact sur les agendas politiques. Et que bien plutôt, l'établissement de tels agendas dépend des pouvoirs en présence et des politiques pratiquées, et tout particulièrement de la capacité d'un ou de plusieurs acteurs de tenir un « discours de la menace » afin par là même de lui donner réalité. En d'autres termes, c'est d'abord dans la conscience individuelle que se construit la menace : ce sont les individus qui perçoivent quelque chose comme une menace. L'étape suivante consiste pour les acteurs de la société prétendument menacée à donner forme à cette menace en la portant sur la scène publique au moyen de la parole et de l'écriture. La menace est alors parée des atours du langage et ainsi transformée en objet de débat public. Ce qui passe le plus souvent par la diffusion d'articles de journaux et de maga-

zines, de documentaires télévisés, et ultimement de livres grand public et de films à large audience.

Dans le contexte des médias de masse, on désigne le processus qui consiste à formuler des problèmes, à trouver des boucs émissaires et à présenter des solutions toutes faites, par le terme de « schème »[1]. Généralement, le choix des « schèmes » a un impact majeur sur l'apparition ou non d'une thématique quelconque sur la scène politique. Typiquement, un « schème de la menace » consiste simplement à identifier quelque chose comme une menace pour la « sécurité ». Les politiques de sécurité sont souvent considérées comme ayant priorité sur tous les autres domaines, et conjointement une politique de sécurité *nationale* est invariablement perçue comme le fondement de toutes les autres politiques de sécurité. Tout cela aboutit à transformer la politique de sécurité et le « schème » associé de la menace en thématiques extrêmement chargées. L'exploitation des concepts politiquement connotés de « sécurité » et de « menace » peut ainsi faciliter l'inscription d'un thème quelconque sur un agenda politique.

Les agendas médiatiques

L'élaboration des agendas médiatiques repose sur ce principe que les médias de masse exercent une influence notable sur la façon dont le public identifie les sujets les plus importants – présupposé théorique conforté par de nombreuses études empiriques. Dans ce domaine, il existe principalement deux types d'approche, l'une qui se concentre sur les élites et l'autre qui s'avère fondamentalement pluraliste. L'approche par les élites se focalise sur le pouvoir politique institutionnel et les décideurs de premier plan, la seconde étend le concept d' « agenda politique » de manière à y inclure des facteurs tels que le ou les agendas des médias eux-mêmes. On insistera ici sur le fait que les médias américains agissent comme la source principale d'information politique des masses – à l'intérieur des États-Unis mais aussi à l'extérieur, et même de manière accentuée du fait du développement de la télévision par satellite et de l'Internet. Ils servent également de

1. Plus subtil et plus explicite, l'anglais *framing* signifie deux choses concomitantes : l'enfermement du discours dans un cadre conceptuel rigide ainsi que le piège idéologique qui se referme sur lui. Ce que veut montrer l'auteure ressortit effectivement à ces deux points, puisqu'elle va montrer que les discours de *fabrication* de la menace cyber-terroriste encadrent et aliènent des pans entiers de la pensée et de l'action politiques *(note du traducteur).*

« courroie de transmission » principale dans la communication des peurs et des désirs du public, tant aux élites politiques qu'aux acteurs gouvernementaux. L'*establishment* traditionnel des médias représente un opérateur de pouvoir majeur au sein de la société contemporaine, qui exerce une influence inégalée sur la diffusion de l'information et de l'actualité. Il agit comme un intermédiaire non seulement entre les masses populaires et le gouvernement, mais aussi au sein même des organes gouvernementaux. On peut aller jusqu'à dire qu'au sein des démocraties où les taux d'affiliation aux partis politiques et où le nombre des adhésions aux organisations communautaires ou civiques sont en déclin, les médias constituent désormais le pouvoir intermédiaire dominant – et occupent une position de monopole dans la fabrication courante de « schèmes de la menace ».

PEUR DE LA TECHNOLOGIE, PEUR DU TERRORISME

Il arrive fréquemment que nos intuitions premières déterminent la manière dont nous appréhendons une situation et la passons au crible de nos préconceptions. De nombreuses recherches en psychologie sociale en concluent que l'inconnu et l'incertain génèrent habituellement peur et anxiété. C'est le fondement psychologique des classiques histoires de fantôme : la peur est plus grande lorsqu'on suspecte quelque chose mais qu'on n'est pas certain de ce qu'il en est. Le terme de « cyber-terrorisme » réunit deux peurs modernes très répandues : la peur de la technologie et la peur du terrorisme. Significativement inconnus et incertains, technologie et terrorisme sont tous deux perçus comme plus inquiétants que toute autre menace connue.

La peur du terrorisme, considérée comme violence incontrôlable, incompréhensible et gratuite, peut paraître à certains comme relativement « normale » ; la peur de la technologie peut-être un peu moins. Cependant, ceux qui ne sont pas familiers de la haute technologie paraissent en subir un impact obscur, complexe, abstrait et indirect. Beaucoup sont ainsi saisis de la crainte que la technologie ne devienne le Maître et l'humanité son Esclave. Couplez cette peur relativement récente aux peurs ancestrales associées à la violence apparemment gratuite du terrorisme, et le résultat obtenu est celui d'un état d'inquiétude véritablement accru. Les médias ont encore alimenté cette peur des tréfonds par le battage médiatique fait autour du concept de « convergence » – idée que toutes les fonctions contrôlées par les ordinateurs personnels se connecteront pour former un

seul et même système si bien qu'au bout du compte notre existence entière sera conditionnée par un réseau informatique tout-puissant et incontrôlable. Convergence accentuée par la dépendance des infrastructures à l'égard des réseaux informatiques et de leur constante alimentation énergétique. Qu'on imagine une attaque contre les réseaux électriques – infrastructures – clés de notre société – et l'effroi atteint son comble. Un tel sentiment se renforce du reste de la prépondérance dans les médias de masse de ce qu'on appelle le scénario du « système-électrique-en-rideau » imaginé par le journaliste et technologue américain Dan Verton.

Le scénario du « système-électrique-en-rideau »

Après le 11 septembre 2001, le spectre de la cyber-terreur a pris un nouveau tour. En 2003, dans un ouvrage intitulé *Verglas : la menace invisible du cyber-terrorisme*[1], Dan Verton analyse la menace que le cyber-terrorisme fait peser sur les marchés de masse. Le premier chapitre du livre décrit une série d'attaques coordonnées, à la fois physiques et virtuelles, lancées contre les infrastructures névralgiques situées au nord-ouest des États-Unis, sur la côte Pacifique. Leurs protagonistes mènent une série d'attentats suicides en utilisant des explosifs conventionnels et de la poudre d'anthrax, introduisent un virus informatique ciblant les serveurs-racines[2] de l'Internet et les téléphones portables, endommageant les pages Web d'un certain nombre d'organismes majeurs d'information et déclenchant une bombe à impulsion électromagnétique. Dan Verton est très explicite quant aux commanditaires : une galerie d'agents para-gouvernementaux comprenant un noyau dur de membres d'Al-Qaida, aidés par des *hackers* russes et par un certain nombre d'employés mécontents des compagnies d'électricité nationales avec des sympathies d'extrême droite. Les effets de ces attaques sont décrits comme durant des semaines en certains endroits, voire des mois en d'autres. Les services d'urgence, les équipements médicaux, les commerces, les banques, les agences gouvernementales, les usines et les entreprises, tous sont dépeints comme subissant des pannes ou des interruptions d'une ampleur susceptible de les contraindre à la faillite.

1. *Black Ice : The Invisible Threat of Cyberterrorism,* McGraw-Hill Osborne Media, 2003.
2. Nom donné aux serveurs névralgiques de l'Internet (au nombre de 13 principaux à travers le monde).

Dan Verton va jusqu'à soutenir qu' « on peut écarter sans problème les opinions de ceux qui affirment que le cyber-terrorisme [...] est impossible ». Assertion acceptable et acceptée parce que dans un monde saturé de médias, tout événement peut être tout à la fois vrai et faux, réel et imaginaire. Verton conclut son scénario par l'observation suivante :

> « Tel est le visage du nouveau terrorisme. C'est un jeu de l'intelligence qui allie les tactiques violentes de l'Ancien Monde aux réalités et vulnérabilités d'un Nouveau Monde *high-tech*. Les jours sont loin où les seules victimes d'une guerre étaient celles qui avaient le malheur de se trouver dans le périmètre d'une déflagration. Le terrorisme concerne désormais le ciblage indirect, planifié et intelligent du maillage des systèmes électroniques d'une nation. »

Simplement prédictif, le fantasme se commue donc en réalité. Et en un temps où l'information se prétend connaissance, il s'avère de plus en plus difficile de distinguer le cyber-terrorisme de ses représentations médiatiques.

L'exagération des scénarios imaginés par Dan Verton ou d'autres peut être d'autant mieux mise en lumière si l'on songe que *blacks out,* pannes et accidents font partie du mode opératoire normal des réseaux informatiques et des infrastructures critiques. Il est bon de garder à l'esprit que les pannes de système – contamination généralisée de l'eau, coupures de courant, interruptions chroniques du trafic aérien, et autres scénarios cyber-catastrophiques – sont des événements qui surviennent régulièrement sans affecter la sécurité nationale. À ce jour, la cyber-*erreur* s'est avérée non seulement plus fréquente mais également plus débilitante que la cyber-*terreur*. En ce qui concerne l'énergie électrique, la plupart des coupures sont dues à des phénomènes naturels comme des conditions climatiques difficiles – dont atteste par exemple l'impact de l'ouragan Katrina sur la Nouvelle-Orléans en 2005. Pourtant, la menace toute fantasmée d'ennemis cyber-experts, politiquement revendicatifs et supposés menacer les infrastructures critiques, continue d'alarmer beaucoup plus de monde que ne le font une erreur d'opérateur ou un phénomène naturel bien réels, quasi quotidiens, non intentionnels et qui entraînent souvent d'importants dommages.

L'IDENTIFICATION DE L'ENNEMI

La question des médiations indispensables à la construction d'un « schème de la menace » exige également qu'on analyse la façon dont sont

désignés des acteurs identifiés comme hostiles. Traditionnellement, les études consacrées aux politiques de sécurité mettent l'accent sur les États ou gouvernements potentiellement menaçants. Mais lors des débats sur le terrorisme et la guerre de l'information, on a insisté sur le fait que des acteurs non étatiques pouvaient également représenter une menace. L'idée que des adversaires anonymes puissent tenter de pénétrer les systèmes d'information à partir de n'importe quel point du monde rompt avec la conception traditionnelle de la sécurité – où l'identité, la localisation et les objectifs de l'ennemi sont connus – et augmente le sentiment de peur et d'insécurité. L'introduction de puissants adversaires non étatiques dans la réflexion sur la sécurité s'apparente à l'ouverture d'une boîte de Pandore car, dans le cyberespace, le nombre de tels ennemis potentiels se trouve virtuellement illimité. Poutant les médias se sont principalement focalisés sur deux de ces ennemis : les *hackers* et les terroristes.

Les « hackers-terroristes »

Avant le 11 septembre 2001, les médias considéraient les *hackers* comme engagés dans des antagonismes les opposant les uns aux autres. Or il y a une histoire de la diabolisation des *hackers,* progressivement considérés comme des délinquants informatiques au cinéma, à la télévision et dans la presse. Personnages d'abord familiers, voire emblématiques, ils ont été au gré de la construction du « schème de la menace » tenus pour de parfaits candidats aux attaques cyber-terroristes.

Un des thèmes les plus populaires et les plus persistants associés aux *hackers* aura été la menace d'infiltration des systèmes militaires les plus sensibles du monde. C'est en 1983, avec *War Games*[1], que le sujet fut pour la première fois porté à l'attention du public. Dans ce film, un adolescent réussit à s'introduire dans l'ordinateur qui surveille et contrôle le système de défense nucléaire américain. Persuadé qu'il ne s'agit que d'un simple jeu, l'adolescent entame une partie avec l'ordinateur, qui estime quant à lui que le jeu est « réel » et qui amorce le décompte d'une Troisième Guerre mondiale. Ce scénario eut un large écho auprès du public américain. Ainsi par exemple, dans le délibéré du jugement le

1. Film de John Badham avec Matthew Broderick, dont le titre n'a pas été traduit lors de son exploitation en France.

condamnant pour intrusion informatique, le célèbre *hacker* américain Kevin Mitnick fut interdit d'accès non seulement à tout ordinateur mais aussi au téléphone, car le juge était convaincu que Mitnick était capable de déclencher une attaque nucléaire à l'aide d'un téléphone !

En 1991, un des épisodes de l'émission télévisée *Geraldo,* consacrée au *hacking*, commença par des extraits du film *58 minutes pour vivre*[1], dans lequel des terroristes prennent le contrôle des ordinateurs d'un aéroport. L'émission inclut également une interview de Craig Niedorf (dit *Knight Lightning*) qui faisait alors l'objet de poursuites judiciaires aux États-Unis pour avoir prétendument reçu le code source des programmes informatiques activant les lignes téléphoniques des services d'urgence. Au cours de la soirée le présentateur, Geraldo Rivera, qualifia à plusieurs reprises Niedorf de « *hacker* fou ». Le Procureur dans le procès de Niedorf se trouvait également sur le plateau. Voici retranscrit un extrait de leurs échanges :

> Rivera. — « Don, comment répondez-vous au sentiment que partagent tant de *hackers,* qu'ils accomplissent une mission de service public en mettant au jour les défauts de nos systèmes de sécurité ? »
>
> Le Procureur. — « Bien sûr, oui ! Tout comme un étudiant qui viole son cothurne sur un campus met au jour les défauts de sécurité de notre système universitaire ! C'est complètement absurde. »

Et au sujet de la condamnation des *hackers* :

> Le Procureur. — « Je ne pense pas du tout qu'ils soient sévèrement punis. Nous avons même du mal à récupérer leur matériel. Je n'en connais pas un seul [qui] ait fait une longue peine de prison [...]. Même la peine infligée à Mitnick, qui est un véritable Hannibal Lecter électronique [...], est demeurée bien en deçà de ce à quoi l'on aurait pu s'attendre au vu de ses agissements. »

À la toute fin de l'émission, Rivera demande au Procureur de donner un bref scénario catastrophe pouvant résulter des activités des *hackers*. Il répond : « Ils rasent tout notre système de communication. Relativement facile. Plus personne ne parle à personne, rien ne bouge, les patients n'obtiennent plus leurs médicaments. On est à genoux. »

Les *hackers* ont mauvaise presse. Pour ce qui est du matraquage médiatique de la menace cyber-terroriste, ce portrait des *hackers* comme ennemis potentiels ne se limite pas au cinéma et à la télévision. On le

1. Film de Renny Harlin avec Bruce Willis (1990). Titre original : *Die Hard 2*.

retrouve également dans la presse, qui les a identifiés à de nombreuses reprises comme les plus probables auteurs de menaces. L'extrait suivant d'un article du magazine *Newsweek* daté de 2003 et intitulé « La destruction de l'Internet »[1], est typique :

> « Si vous souhaitiez écrire un *thriller* de science-fiction sur le jour où l'Internet s'effondrerait, vous débuteriez avec un *geek*[2] informatique. Armé de son seul ordinateur et d'une connexion Internet à haut débit, il lâcherait un virus informatique qui s'en irait se répliquer rapidement et lui donnerait le contrôle, en l'espace de quelques minutes, de millions d'ordinateurs personnels et de serveurs à travers le monde. Cette armée de drones lancerait alors une attaque silencieuse et soutenue contre les ordinateurs centraux des infrastructures de base de la vie moderne. L'attaque ne semblerait tout d'abord être qu'un dérangement passager : la circulation des e-mails s'arrêterait et la navigation sur le Net deviendrait impossible. Puis les problèmes s'étendraient ensuite aux services qui ne sont qu'indirectement liés à l'Internet : les guichets automatiques s'arrêteraient, les appels des numéros d'urgence ne seraient plus redirigés vers les commissariats de police ou les services ambulanciers, les systèmes de réservation de train et d'avion s'effondreraient. Quelques heures plus tard, ce ralentissement affecterait les systèmes critiques, les ordinateurs contrôlant les réseaux électriques, le trafic aérien et le téléphone. »

Selon les auteurs de ce scénario, ces pannes en cascade ne sont pas seulement d'envergure régionale ou nationale mais bien mondiale. Et en l'espace de quelques lignes, leurs protagonistes passent du statut de *hackers* à celui de *geeks* puis de « terroristes ». Le problème reste que même si les *hackers* réussissaient un tel exploit, ce ne serait pas du cyber-terrorisme – à moins que leurs objectifs ne fussent politiques. La plupart des journalistes ou bien ignorent cette nuance ou bien la récusent, au point que la presse va jusqu'à qualifier de « cyber-terrorisme » certains délits informatiques véniels.

Envoyer des mails pornographiques à des mineurs, poster un contenu injurieux sur le net, dégrader des pages Web, utiliser un ordinateur pour causer des pertes s'élevant à 300 €, voler les informations confidentielles d'une carte de crédit, publier sur le Net des numéros de carte de crédit, rediriger de manière clandestine d'un site sur un autre – voilà ce qui dans beaucoup d'articles de presse constitue des actes de cyber-terrorisme ! Et pourtant, aucune de ces actions n'aurait pu être considérée comme terroriste – certaines d'entre elles ne sont même pas criminelles – si elle n'avait

1. Titre original : *Bringing Down the Internet*.
2. Terme désignant le passionné d'informatique avec une connotation parfois laudative (expertise), et parfois péjorative (fanatisme, délinquance).

été accomplie au moyen d'ordinateurs. Il est vrai que le terrorisme est notablement difficile à définir. Cependant l'ajout d'ordinateurs à un simple délit conventionnel ne le fait certainement pas tomber dans cette catégorie. Quelle est donc la fonction de tels articles ? De construire un domaine de définition propre à la catégorie de « cyber-terrorisme » – ce qui est capital, dans la mesure où aucun acte cyber-terroriste « véritable » n'a au sens rigoureux du terme jamais été perpétré. Pour rendre crédible le schème de la menace cyber-terroriste, les scénarios envisagés exploitent donc toutes sortes de versions paroxystiques d'une cyber-terreur enracinée dans le personnage de l'adolescent *hacker*.

On peut certes difficilement considérer les différentes façons de détourner les technologies de l'information comme de réelles menaces pour l'existence des États souverains. Malgré cela, le discours dominant entretient l'idée que des intrus malveillants – de jeunes *geeks* informatiques formés sur le tas... – font peser des menaces potentiellement catastrophiques sur la sécurité nationale ou économique. D'où la question cruciale de savoir comment des adolescents obsessionnels et autodidactes pourraient triompher des sécurités conçues par les gouvernements et les entreprises ayant dépensé ensemble des milliards d'euros pour protéger leurs systèmes et sévir contre les cyber-criminels ! Plus récemment, en fait, les médias ont révisé leur discours du « *hacker*-terroriste » – de moins en moins convaincant – et, au détour du 11 septembre 2001, lui ont substitué l'approche du « terroriste-*hacker* ».

Les « terroristes-hackers »

Les attentats du 11 septembre 2001 ont conduit à un changement radical dans la perception des menaces, autant de celles provenant du terrorisme conventionnel que de celles concernant le cyberespace. Dans le sillage immédiat des attaques, une prolifération d'articles de presse ont traité de la menace cyber-terroriste. Une recherche dans les archives de Lexis-Nexis montre que dans le *Washington Post* ou le *New York Times,* par exemple, les références au cyber-terrorisme ont doublé à la suite du 11 septembre 2001. Beaucoup se sont à l'époque posé la question : « Sommes-nous à l'aube du cyber-terrorisme ? »

Une fois qu'Oussama Ben Laden et Al-Qaida ont été identifiés comme les commanditaires des attentats du 11 septembre 2001, un flot impres-

sionnant d'articles est venu suggérer qu'ils s'attelleraient désormais à la planification d'une attaque cyber-terroriste de grande ampleur. Ainsi, alors même qu'il n'y avait aucune preuve tangible qui permît de mesurer le degré de maîtrise des technologies de l'information par Al-Qaida, un nombre croissant de personnes en est venu à tenir cette menace pour substantielle – et à la craindre ! Ainsi s'emballa un hypermédiatique cercle vicieux, les médias dramatisant les estimations des services secrets, les hommes politiques reprenant à leur tour des citations des médias, les relayant aussitôt auprès d'espaces médiatiques tiers, et ainsi de suite. En un rien de temps, des peurs infondées s'étaient commuées en pronostics avérés !

En novembre 2001 parut dans le magazine *Information Security* un article qui combla le fossé séparant le « possible » ou le « probable » du « très vraisemblable » :

> « Quand bien même il faudrait attendre de voir des groupes terroristes tels que le Hezbollah, le Hamas, Abu Nidal ou Al-Qaida utiliser le *hacking* et des logiciels malveillants et prendre pour cible de nos infrastructures critiques, leur propre dépendance vis-à-vis des technologies de l'information et leur expertise informatique constituent un signal d'alerte évident. Tandis que jusqu'à maintenant les dégâts causés par les *hacktivistes*[1] – et même par les cyber-terroristes – ont été minimes, les experts en sécurité prévoient que l'infrastructure des technologies de l'information de la nation sera *très vraisemblablement* une cible dans l'avenir. »

En outre, un article paru dans *Newsweek* en mai 2002 titrait : « Le cyber-terrorisme islamique : une simple question de temps. »[2] À la fin du mois de juin 2002, Roger Cressey, à l'époque chef du Bureau présidentiel de protection des infrastructures critiques, affirma une chose remarquablement similaire : « Al-Qaida a passé plus de temps à repérer nos vulnérabilités dans le cyberespace qu'on ne le pensait auparavant. On ne se pose plus la question de savoir *si* une attaque doit avoir lieu, on se pose la question de savoir *quand* elle aura lieu. » Cette déclaration a provoqué en 2002 une averse de reportages de presse fantasmant sur les prétendus plans cyber-terroristes d'Al-Qaida[3].

1. Nom donné à ceux qui allient l'expertise informatique à l'activisme politique.
2. Titre original : « Islamic Cyberterror : Not a matter of if, but of when ».
3. Parmi eux, on retiendra : « Report : US Fears Possible Al-Qaeda Cyber-Attacks », Reuters, 27 juin ; « Cyber-Attacks by Al-Qaeda Feared », Barton Gellman in *Washington Post,* 27 juin ; « US Fears Al-Qaeda Hack Attack », Kevin Anderson, in *BBC News Online,* 27 juin ; « Qaeda Cyberterror Called Real Peril », Barton Gellman in *International Herald Tribune,* 28 juin ; « US Fears Al-Qaida Will Hit Vital Computer Networks », Julian Borger, in *The Guardian* (UK), 28 juin.

Paru dans le *Federal Computer Week* du 25 juillet, un article de William Matthew, « Al-Qaida : l'alarme cybernétique »[1], reprenait un pronostic de Lamar Smith, membre de la Chambre des représentants (Texas), sur le fait qu' « il y [avait] 50 % de chances pour que la prochaine attaque terroriste d'Al-Qaida frappant les États-Unis [comprît] une cyber-attaque ».

Le basculement opéré dans le « schème » de la menace cyber-terroriste avec le passage des « *hackers*-terroristes » aux « terroristes-*hackers* », illustre deux choses : la *première* est que la défense et le combat contre les menaces de sécurité sont clairement facilités lorsqu'on est à même d'en identifier les auteurs. Le processus d'introduction d'un « schème de la menace » dans l'agenda politique est manifestement simplifié par la capacité d'identifier le ou les acteurs constituant la menace. Les menaces structurelles ont plus de difficulté à attirer l'attention que celles qui sont adossées à des protagonistes « connus ». Ainsi, alors que l'identification de la menace cyber-terroriste à une catégorie amorphe telle que celle du *hacker* est plus pertinente, la capacité d'identifier Oussama Ben Laden ou Al-Qaida comme sources de la menace cyber-terroriste est clairement privilégiée. *Deuxièmement,* certains événements tragiques ont certainement eu un impact sur l'écho produit par ce « schème de la menace ». Les événements du 11 septembre 2001 ont servi de catalyseur en revivifiant le discours sur la menace cyber-terroriste et en particulier l'idée du « terroriste-*hacker* ».

CONCLUSION

Le tableau de la menace terroriste a donc été peint par les médias américains et a produit ses effets. Lesquels ? Bien que ce qu'on appelle la « cyber-hystérie » ait pu tirer son origine de sources fantasmatiques, il est également clair que ses conséquences ont été bien réelles.

Avant les événements du 11 septembre 2001, seul un petit nombre d'universitaires et de personnalités avaient insisté sur le risque d'une attaque terroriste massive et *conventionnelle* sur les États-Unis. Le risque en avait été écarté par les médias qui avaient choisi au contraire de se concentrer sur le cyber-terrorisme. Les décideurs clés avaient donc été beaucoup plus sensibilisés à cette seconde menace qu'à la première. Voici

1. Titre original : « Al-Qaeda Cyber Alarm Sounded ».

ce que Marcus Sachs[1] déclarait en 2003 à propos de la convergence, parmi les membres du personnel politique, de la peur du terrorisme et de la peur de la technologie :

> « Au gouvernement fédéral, nous avons été très choqués de voir que les attaques ne sont pas venues du cyberespace [...]. Selon nos informations de l'époque, le scénario le plus probable était celui d'une attaque venant du cyberespace, et non celui d'avions commerciaux s'écrasant contre des bâtiments [...]. Nous avions passé énormément de temps à nous préparer à une cyber-attaque, non à une attaque physique. »

L'intuition qui aide à déterminer quels sujets possèdent une pertinence politique s'avère assurément un processus continu qui requiert de s'intéresser à la manière dont des « schèmes de menace » sont créés, entretenus et modifiés de façon discursive. C'est pourquoi il faut insister sur les processus par lesquels les problèmes de sécurité (nationale) émergent dans le public, et le rôle central que jouent les médias dans ces processus. La communication politique et le climat de menace induit modèlent ensemble l'information disponible et les diverses manières dont elle est utilisée non par les gens ordinaires seulement, mais aussi par les élites politiques – pour penser la politique, précisément, et la sécurité nationale.

Démontrer les effets de l'influence des médias sur le public et sur les décideurs est toujours chose difficile, en raison des dynamiques complexes et indirectes qui sont impliquées. Il est toutefois évident que les médias américains ont par leurs discours très bien réussi à donner une réalité au cyber-terrorisme. En s'adossant d'abord à des scénarios permettant de générer une sorte d' « hyper-réalité » ; en dressant ensuite le portrait des *hackers* comme de véritables menaces pour la sécurité nationale ; en élargissant enfin le domaine de définition du concept de cyber-terrorisme. Tout cela concurremment à l'ouverture d'une fenêtre d'opportunité politique suscitée par les événements du 11 septembre 2001, qui permit de projeter Oussama Ben Laden et Al-Qaida comme de probables futurs cyber-terroristes. Le matraquage médiatique a ainsi permis d'établir une connexion fatale (imaginaire) entre les réseaux virtuels et les infrastructures physiques critiques, laquelle pourtant n'a jusqu'à ce jour que très peu de substance réelle.

Conclusion qui n'est peut-être pas si dérangeante qu'il y paraît au premier abord. Pourquoi ? Peut-être parce que tous les différents scénarios

1. Membre à la Maison-Blanche du Service de la sécurité dans le cyberespace ainsi que du Bureau présidentiel pour la protection des infrastructures critiques.

apocalyptiques, les simulations télévisées et les élucubrations quant à la plus grande létalité des attaques virtuelles que des attaques nucléaires auraient en fait assuré qu'un « Pearl Harbour virtuel » ne se matérialiserait jamais – encore une analogie adorée des journalistes de presse et de télévision ! La raison en est que la crainte du cyber-terrorisme s'est tellement généralisée et avec tant de succès que, si une telle attaque devait survenir en bonne et due forme, elle ne pourrait jamais remplir les attentes du public : toute attaque cyber-terroriste réelle qui ne répliquerait pas et même n'excéderait pas les simulations, qui ne produirait pas le chaos généralisé et les pertes humaines massives tant attendues, perdrait purement et simplement sa dignité et sa capacité de susciter la crainte ou même l'intérêt du public.

(Traduction de l'anglais par Clémentine Chaigneau, revue par Paul Mathias.)