TECHNOLOGIES ET SÉCURITÉ APRÈS LE 11 SEPTEMBRE 2001

PAR

BERTRAND WARUSFEL (*)

Technologie et sécurité entretiennent depuis longtemps une relation complexe et ambivalente : l'aspiration à une sécurité croissante nourrit perpétuellement le progrès technique, mais – inversement – chaque nouvelle innovation technologique significative engendre ses propres insécurités et peut fournir des moyens nouveaux pour déjouer des dispositifs de sécurité existants. Et cette relation paradoxale vaut autant pour la sécurité privée (sécurité automobile, risques d'accident domestique) ou industrielle (risques d'accidents industriels ou écologiques) que dans le champ de la sécurité internationale.

De ce point de vue également, les attentats de New York et de Washington du 11 septembre 2001 et l'enchaînement des événements qui s'ensuivit (en particulier en Afghanistan) apparaissent révélateurs, non pas tant d'une nouvelle ère des relations internationales, que des paradoxes latents de notre société technologique mondialisée.

LA DIMENSION TECHNIQUE DES ATTENTATS DU 11 SEPTEMBRE

Passée l'émotion des premiers jours, on a beaucoup discuté de l'appréciation qu'il convenait de porter sur l'événement et sur les modalités des actes terroristes que chacun avait visualisés en quasi simultané par la voie des médias. Étions-nous en face d'un « hyperterrorisme » (1) rompant en puissance de destruction et de communication avec les modalités préexistantes du terrorisme de la fin du XX^{e} siècle ? Assistions-nous, plutôt, à un dernier avatar du terrorisme aérien, inventé par les mouvements palestiniens radicaux aux lendemains de la guerre des Six Jours ? Les analyses les plus variées ont immédiatement été proposées et l'un des aspects qui a donné lieu à débat a été le contraste apparent entre la rusticité volontaire des moyens utilisés par les commandos pour prendre le contrôle des avions de

(*) Maître de conférences à la Faculté de Droit de l'Université René Descartes (Paris V) et conseil en propriété industrielle.

(1) Sur le concept et le néologisme d'« hyper-terrorisme », *cf.* l'ouvrage de François HEISBOURG et de la Fondation pour la recherche stratégique, *Hyperterrorisme : la nouvelle guerre*, Odile Jacob, 2001.

ligne et les détourner sur leurs cibles (des armes blanches « par destination » tel que, semble-t-il, des instruments courants ou peu repérables : cutters, limes à ongle...) et les effets considérables obtenus en terme de destructions et de pertes humaines (à des niveaux que l'on croyait ne pouvoir connaître que dans le cas d'armes très puissantes, voire de destruction massive) (2).

Il est donc légitime de chercher à savoir si les attentats du 11 septembre appartiennent ou non à ce terrorisme « *high-tech* » dont beaucoup annonçaient l'émergence (mais plutôt sous la forme d'actes terroristes nucléaires ou biologiques) ou si, au contraire, l'un des centres de l'Occident industriel et technologique a été pris à revers par une agression a-technique qui emprunterait surtout à des pratiques anciennes basées sur le fanatisme personnel ou religieux. Et la réponse a une telle question n'est pas neutre : valider la seconde option revient à accréditer l'émergence d'une véritable « guerre des civilisations », tandis que la première nous incite à continuer à réfléchir à l'intérieur même du modèle de référence occidental et industriel.

Admettons d'emblée qu'effectivement, il ne semble pas (dans la limite de ce que l'on sait, trois mois après, des résultats de l'enquête) que les moyens matériels engagés par les équipes de terroristes pour commettre les attentats aient été technologiquement sophistiqués en eux-mêmes. On connaît d'ailleurs l'une au moins des raisons essentielles de cette modestie : il convenait de pouvoir franchir aisément les contrôles et les portiques de sécurité des aéroports d'embarquement, ce qui limitait les possibilités d'utiliser des équipements techniques particuliers (dont la présence aurait pu éveiller les soupçons et, vraisemblablement, faire réagir les détecteurs automatisés). L'absence de tout équipement métallique et/ou électronique détectable lors de la fouille des passagers et des bagages retire-t-elle pour autant toute dimension technique à ce qui s'est produit au-dessus de Manhattan et de Washington ?

Ce serait mal comprendre ce que Jacques Ellul dénommait un « *phénomène technique* » (3). La technique ne se réduit pas aux seuls objets matériels issus de la mise en œuvre industrielle de certaines technologies modernes. Est technique tout ce qui procède de manière systématique dans le souci de rechercher l'efficacité maximale au regard des moyens employés (ce que l'on nomme justement « l'économie de moyens ») et en mettant à contribution les connaissances scientifiques acquises quant au fonctionnement des lois de la nature et/ou de la société. Et de ce point de vue, la campagne d'attentats

(2) Un article paru dans la revue du MIT résume bien dans son titre et son sous-titre l'incrédulité qu'ont éprouvée de nombreux Américains devant l'apparente rusticité de l'attaque dont ils venaient d'être victimes : Edward Tenner, « The Shock of the Old – On September 11, a nation primed for a futuristic attack failed to foresee a low-tech assault. Why ? », *Technology Review*, décembre 2001.

(3) « *Le phénomène technique est donc la préoccupation de l'immense majorité des hommes de notre temps, de rechercher en toutes choses la méthode absolument la plus efficace* » (Jacques Ellul, *La Technique ou l'enjeu du siècle*, Paris, 1954, réed. Economica, 1990, pp. 18-19).

menée aux États-Unis durant la matinée du 11 septembre 2001 nous paraît être indiscutablement une opération technique (4).

Cette dimension technique de l'opération se situe d'abord au niveau de sa planification et de sa coordination. Organiser le déroulement quasi simultané de quatre détournements de vol au départ de plusieurs aérodromes et faire converger les avions détournés sur certaines cibles (en particulier les deux avions d'*American Airlines* qui iront percuter successivement les deux tours du World Trade Center, à dix-huit minutes d'intervalle) nécessite une préparation poussée et minutée. Celle-ci a dû obliger les organisateurs à différents travaux préparatoires, tels que repérages dans les aéroports de départ, étude des horaires de vol, minutage des temps de vol, repérage des cibles et de leur environnement aérien, préparation des plans de vol après le détournement. Puis il a sans doute été nécessaire qu'un coordonnateur-régulateur suive le déroulement des opérations pour en assurer le déclenchement synchronisé selon le planning fixé. Et comme l'ont relevé immédiatement certains experts américains, l'opération était entièrement basée sur la mise en œuvre du « concept sophistiqué de redondance », qui procurait statistiquement le maximum de garantie de résultat (5). Si l'on ajoute à cela que, plus en amont de l'événement, il a été nécessaire d'acheminer et de regrouper en toute discrétion sur le territoire américain plus d'une dizaine de personnes, on comprend bien qu'une telle opération repose nécessairement sur une véritable « gestion de projet », au sens où l'on entend ce concept dans le cadre du *management* industriel.

La technique ne paraît pas seulement présente dans la phase préliminaire de l'opération, elle a été certainement également sollicitée pour son exécution elle-même, bien que l'on ait moins de certitude à ce niveau en raison de la discrétion qui entoure les enquêtes en cours. Deux moments clefs paraissent requérir une certaine technicité : tout d'abord, le passage des contrôles de sécurité au départ des vols intérieurs (la dissimulation d'objets contondants dans les bagages à main ou sur le corps des terroristes exposait éventuellement ceux-ci à une découverte lors d'une fouille ou du passage au détecteur; il a donc sans doute fallu observer les pratiques de détection et de fouille, la sensibilité des appareils employés afin de mettre au point une technique de camouflage appropriée); ensuite, une fois la prise de contrôle de l'appareil réalisée sous la contrainte après le décollage, il convenait – évidemment – que les terroristes puissent modifier la trajectoire des vols afin d'approcher le plus près possible de leurs objectifs, puis – une fois en vue de ceux-ci – diriger manuellement l'appareil directement sur ceux-ci.

(4) Dans le même sens, Thérèse DELPECH, « The Imbalance of Terror », *The Washington Quarterly*, hiver 2002, p. 33.

(5) « *The terrorists were extremely organized, sophisticated and well-funded, security experts said. They used the sophisticated concept of 'redundancy', incorporating several separate, coordinated attacks that allowed the operation to continue even if one group was detected, according to security experts* » (Kristen PHILIPKOSKI, « Where Was U.S. Intelligence ? », *Wired*, 12 September 2001).

Tout cela ne demandait sans doute pas de compétences très pointues en matière de pilotage, mais néanmoins un certain entraînement et une connaissance préalable des principaux dispositifs techniques disponibles sur un avion de ligne moderne (propulsion, guidage, mais aussi navigation et radio). C'est la raison pour laquelle plusieurs des personnes identifiées comme ayant participé aux détournements tragiques auraient pris des cours de pilotage pour se familiariser avec l'ensemble des connaissances et des pratiques indispensables. Mais, là encore, la mise en œuvre efficace (si l'on peut parler ainsi malgré l'horreur des conséquences, puisque la majorité des cibles visées paraît avoir été atteintes) de ces techniques de dissimulation puis de pilotage, a très vraisemblablement nécessité de la part de leurs exécutants une préparation minutieuse et coordonnée au cours de laquelle différents scénarios ont dû être prévus et répétés, de façon à garantir un résultat efficace.

Ajoutons enfin que les objectifs et la logique même de ces opérations révèlent une dimension technique très forte. Il fallait au moins anticiper partiellement la nature des dégâts susceptibles d'être causés par de tels impacts (ce qui obligeait, là encore, à étudier au moins sommairement les effets de chocs sur les structures de tels bâtiments [6]). Mais il n'est pas exclu que le choix des cibles n'ait pas uniquement été effectué sur des bases simplement symboliques, mais aussi en fonction du potentiel de perturbation que de telles destructions étaient susceptibles de produire : à Manhattan, la destruction des tours jumelles du World Trade Center était de nature à fragiliser l'activité de nombreux acteurs du monde des affaires et de la finance internationale, ainsi qu'à désorganiser les réseaux informatiques et de communication de la principale métropole économique mondiale; à Washington, s'il était plus illusoire d'espérer toucher directement les centres vitaux de commandement de l'appareil militaire américain, il n'est exclu que la Maison Blanche ait été l'un des objectifs initiaux et que son éventuelle destruction partielle ait été programmée pour – au-delà du traumatisme politique majeur – handicaper les capacités de réaction de l'exécutif fédéral durant une certaine période.

Il paraît donc parfaitement justifié de considérer que les attentats du 11 septembre (sans parler de l'attentat – apparemment précurseur – contre le Commandant Massoud le 9 septembre, qui nécessitait également une pla-

(6) Plusieurs professeurs d'architecture du MIT estiment que « *the terrorists probably knew what they were doing. If you had a way of compromising any significant number of exterior columns and then attacking the inner tube simultaneously by essentially laying in a bomb at the middle of the building, that's probably one of the only ways to bring those buildings down, says John Fernandez, an assistant professor in the architecture school. Even the hijackers decision to aim for the area of the towers 90th floors may have been calculated. If the planes had hit at higher floors, conceivable that the progressive failure would not have happened, says Buyukozturk. Every aspect of it shows us that this was a very coordinated, knowledgeable, though terrible act* » (« Fathoming the Towers' Structural Failure », *Technology Review*, September 27, 2001). Cela n'est pas contradictoire avec le fait que – comme tendrait à le montrer l'enregistrement vidéo d'une conversation d'Oussama Ben Laden, produit par les autorités américaines au début du mois de décembre – le résultat a pu être supérieur aux prévisions initiales des concepteurs des attentats.

nification et une technique bien éprouvée) sont bien le résultat d'une opération techniquement planifiée et mettant judicieusement à profit les capacités et les vulnérabilités techniques propres à une société industrialisée et ouverte comme les États-Unis. Loin d'être une opération rustique mettant en œuvre les seuls instruments d'un lointain Moyen Age obscurantiste, cette campagne d'attentats s'est simplement contentée d'aller prendre les moyens techniques sur place : pour frapper fort et précis il fallait un vecteur, celui-ci est disponible sur chaque aéroport sous la forme d'un avion de ligne à turboréacteur; pour réaliser une destruction massive, il convient de viser une vaste concentration d'individus dans un volume limité et aux structures fragiles, comme par exemple à l'intérieur de ces grand *buildings* hypertrophiés construits volontairement dans un souci de grande légèreté (pour éviter les effets d'un poids trop importants des bâtiments) et de flexibilité (pour éviter les risques de trop grande prise au vent).

En d'autres termes, il s'agit bien là d'un terrorisme technologique, puisque c'est en assimilant et en récupérant lorsque cela était possible, les potentialités techniques de leurs cibles et de leurs adversaires, que les concepteurs de cette opération ont réussi à obtenir – au moindre coût – le niveau terrible et spectaculaire de résultat que l'on sait. Il n'est dès lors pas paradoxal, contrairement à ce que certains ont prétendu, que la majorité des exécutants de l'opération (voire sans doute des présumés responsables, y compris Oussama Ben Laden qui a dirigé une entreprise de travaux publics) ait été de formation technique et universitaire. Cela pourrait même nous amener à nous interroger sur les possibles implications indirectes, en amont, de l'équipe terroriste concernée par une éventuelle organisation étatique, rompue aux techniques opérationnelles modernes, mais cela dépasse ici notre propos et notre connaissance du dossier.

La démonstration des limites des technologies de sécurité

Si donc les attentats du 11 septembre révèlent à l'analyse une dimension technique incontestable, il faut également admettre qu'ils ont eu pour effet de démontrer avec éclat les vulnérabilités de nos sociétés ouvertes et développées et, particulièrement, les limites des technologies de sécurité que celles-ci se flattent de déployer préventivement pour contrer les principales menaces majeures.

Cette faiblesse a été patente à deux niveaux de la chaîne : sur le plan matériel, les moyens de filtrage et de sécurité mis en œuvre sur les aéroports et à bord des appareils de ligne ont été nettement contournés; sur le plan de l'information, les dispositifs de renseignement et de surveillance n'ont pas permis de détecter à temps une éventuelle menace terroriste et de mettre en alerte les autorités compétentes. Pourtant, dans les deux cas, on

pouvait penser que les principaux pays industrialisés (et au premier rang les Etats-Unis) y consacraient suffisamment d'investissements et de moyens. Mais à y regarder de plus près, cet optimisme n'avait jamais été complètement justifié.

S'agissant de la sécurité aérienne, les nombreuses techniques de contrôle de toute sorte (vidéosurveillance, fouille, détection automatique du contenu des bagages, contrôle de police, procédures d'enregistrement...) ne doivent pas cacher que, confronté à un accroissement massif du volume du transport aérien mondial (7), leur rôle reste essentiellement dissuasif (augmenter statistiquement le risque d'une éventuelle détection, ce qui doit pousser les candidats terroristes à la prudence et compliquer leurs actions) et largement psychologique (rassurer les passagers). Et les interventions des centres de contrôle aérien pour tenter d'alerter en cas de détournement et d'intervenir avant un *crash* volontaire, sont considérés par les spécialistes comme quasiment inenvisageables étant donné l'importance du trafic et la vitesse des avions (8). De plus, on sait depuis plusieurs années (et, en particulier, depuis l'accident du Boeing de la TWA en 1996) que la banalisation du transport aérien aux Etats-Unis et la concurrence acharnée des compagnies sur ce marché ont contribué à ce que le niveau moyen de sécurité des aéroports et des compagnies aériennes américaines soit plutôt inférieur à ce qu'il est en Europe (9).

S'agissant des moyens de renseignement, on connaît les efforts considérables que les Etats-Unis (et dans une moindre mesure certains de leurs partenaires européens) ont consenti depuis des décennies pour être en mesure de détecter de manière préventive toute menace, en particulier par l'utilisation intensive de moyens techniques d'interception (tels que ceux gérés par la National Security Agency et mis en commun avec d'autres pays anglo-saxons dans le cadre de l'accord UKUSA). Mais nous avions déjà indiqué dans ces mêmes colonnes, l'an dernier, que si l'on pouvait considérer comme « *avéré* » l'existence d'un tel programme transnational de renseignement électronique (parfois dénommé, de manière simpliste « Echelon »), « *l'incertitude plane, en revanche, sur les réelles capacités technologiques d'un tel système* » (10). Ce qui s'est passé à New York et à Washington ne vient donc qu'apporter la preuve, non de l'inefficacité globale de ce type de système,

(7) Selon l'International Air Transport Association, le trafic mondial devrait passer de 571 millions de passagers en 1998 à 1,1 milliard en 2015.

(8) C'est en tout cas ce qu'affirment les contrôleurs aériens eux-mêmes (soucieux de ne pas se faire imposer de nouvelles contraintes liées à la sécurité) : « *compte tenu des connaissances actuelles, il s'avère impossible de renforcer davantage la sécurité sur les écrans de contrôle* » (propos de Marc BAUMGARTNER, vice-président « Europe » de l'Ifatca, Fédération internationale des associations de contrôleurs aériens, reproduit dans *La Tribune*, 19 septembre 2001).

(9) *Cf.*, par exemple, l'enquête de *Time* après le *crash* de la TWA : « Keeping the Skies safe : The US has not been as diligent as other nations at putting tough security measures into place », *Time Magazine*, 26 juillet 1996, pp. 28-31.

(10) Franck LEPRÉVOST / Bertrand WARUSFEL, « Echelon : Origines et perspectives d'un débat transnational », *Annuaire Français des Relations Internationales*, n° 2, 2001, p. 886.

mais – à tout le moins – du fait qu'il n'est pas possible d'espérer qu'un simple dispositif technique (si puissant soit-il) puisse détecter automatiquement et suffisamment à l'avance toute menace extérieure.

A cela s'ajoute très certainement, comme beaucoup l'ont relevé, les effets pervers de la priorité donnée depuis dix ans au *clean Sigint* (le renseignement électronique « propre » [11]) par opposition aux dangereuses compromissions que pouvait entraîner la manipulation de sources humaines. Faute de recruter suffisamment d'agents dans les milieux hostiles, les services de sécurité américains se sont sans doute trop fiés à la puissance supposée de leurs moyens électroniques, censés tisser autour de la sécurité nationale des Etats-Unis le même type de filet de protection que celui que le projet de bouclier anti-missile aurait vocation à assurer (sur le papier!) face aux menaces air-sol.

Mais cette défaite du renseignement technologique américain est d'autant plus caractéristique que l'essentiel de la menace était déjà largement identifié. Pour s'en tenir à l'information ouverte accessible au grand public, la presse américaine avait relaté avec beaucoup de détails les avancées de l'enquête du FBI après les attentats contre les ambassades américaines au Kenya et en Tanzanie en 1998. Et dès cette époque, non seulement l'identification d'Oussama Ben Laden était tenue pour certaine (comme commanditaire des attentats contre les ambassades et de celui du premier attentat contre le World Trade Center en 1993), mais encore il était indiqué que l'on s'attendait de sa part à une attaque surprise contre une grande ville américaine (Washington ou New York) et que l'un des principaux coordinateurs de l'attentat de 1993 à New York tombé entre les mains du FBI, Ramzi Youssef, avait été arrêté alors qu'il projetait d'organiser plusieurs détournements d'avion simultanés sur le territoire américain (12).

Ainsi donc, toute la technologie sécuritaire mise en œuvre par une nation réputée pour être parmi les plus efficaces dans le maniement de ces instruments n'a servi à rien pour détecter à temps et prévenir des actes dont on connaissait depuis plusieurs années le danger et dont on soupçonnait jusqu'aux cibles potentielles. Au contraire, cette technologie sophistiquée qui permet de disposer très aisément de moyens de communication et de transport performants, a été utilisée avec ruse et détermination par un adversaire décidé à se servir de ce que les économistes et les sociologues appellent par-

(11) Selon l'expression de Frank J. CILLUFFO / Ronald A. MARKS / George C. SALMOIRAGHI, « The Use and Limits of US Intelligence », *The Washington Quarterly,* vol. 25, n° 1, hiver 2002, p. 62. Dans le même sens en France, Christian HARBULOT, « La fin du mythe du renseignement technologique », 13 septembre 2001 (accessible sur le site http://news.zdnet.fr).

(12) « Inside the Hunt for Oussama », *Time Magazine*, 21 décembre 1998, pp. 32-35. Dans cet article, on apprenait également que R. Youssef avait dit aux fonctionnaires du FBI que s'il avait à sa disposition un peu plus d'argent, il recommencerait à attaquer les tours du World Trade Center (« *Next time, if i have more money, I'll knock it down* », p. 33) et que, du côté du gouvernement fédéral, on avait pris la menace suffisamment au sérieux pour que M^me^ Janet Reno (alors Attorney General) organise en octobre 1998 un exercice d'état-major simulant une attaque terroriste sur Washington (*cf.* p. 32).

fois les « effets de réseau » propres aux sociétés technologiques modernes (ici, les effets démultiplicateurs liés au détournement des réseaux de transport aérien, puis les effets médiatiques dus à l'exploitation en direct de la séquence des attentats successifs) et à mener ce que nous avions décrit, pour notre part, comme des « *stratégies indirectes de perturbation* » (13). Ainsi que le dit très justement Dominique David dans un récent article consacré à ces attentats de septembre 2001 : « *la vulnérabilité globale des sociétés sophistiquées croît plus rapidement que les moyens techniques d'y parer* (...) *Pour frapper un pays développé de telle sorte qu'un coup limité ait un large effet, il faut refuser d'entrer sur le champ d'affrontement où ce pays contrôle une écrasante palette de moyens, et le frapper là où sa sophistication est une faiblesse et non une force* (...). *La technique est donc le problème stratégique, et non le moyen de résoudre ce problème* » (14).

Ce constat amer sur les limites naturelles de toute technologie sécuritaire dans une société ouverte va-t-il pour autant faire évoluer les visions stratégiques et réviser certains jugements pour l'avenir ? Cela n'est malheureusement pas certain.

Quelques leçons du 11 septembre pour les sociétés technologiques

Si l'on considère donc les attentats du 11 septembre 2001 non comme une action artisanale mais – au contraire – comme une opération technique sophistiquée (malgré l'apparente modestie des moyens matériels employés) et spécifiquement destinée à contourner les technologies de sécurité occidentale et à en exploiter certaines faiblesses, il conviendrait d'en tirer quelques enseignements pour l'avenir. Pour notre part, nous voudrions nous contenter d'en évoquer trois principales.

Premièrement, il a été démontré que la vulnérabilité intrinsèque des sociétés technologiquement avancées était exploitable par un adversaire déterminé pour créer de fortes perturbations. Ce thème de la vulnérabilité des sociétés post-industrielles en réseau n'est pas nouveau. Dès la fin des années soixante-dix, un fameux rapport du ministère de la Défense suédois étudiait la « *vulnérabilité de la société informatisée* » (15). Mais si la perspective était considérée depuis longtemps par les experts, l'on n'avait eu peu d'occasion de constater à quel point les dispositifs socio-économiques les plus communs (mais aussi les plus technologiques) comme les transports, les

(13) *Cf.* Bertrand Warusfel / Patrick Folléa, « Contribution à une réflexion sur les stratégies indirectes », *Stratégique*, n° 4, Fondation pour les Études de défense nationale, 1987, pp. 39 et s.

(14) Dominique David, « 11 septembre : premières leçons stratégiques », *Politique étrangère*, octobre-décembre 2001, pp. 770-771.

(15) *The Vulnerability of the Computerized Society* – Considerations and Proposals' Report by a Swedish Government Committee (Sårbarhetskommiteé), 1979 (titre suédois : « ADB och samhällets sårbarhet, övervaganden och forslag »).

systèmes de communication, les centres d'affaires – pouvaient constituer des cibles idéales (car faciles d'accès et difficiles à sécuriser du fait de leur large ouverture au public). Et si la suite des événements a montré que, fort heureusement, de telles actions ne sont pas susceptibles de désorganiser durablement la vie collective d'une grande cité, on a aussi constaté que les dégâts psychologiques et politiques sont, en revanche, susceptibles d'être considérables (ce qui était sans doute le but essentiel recherché).

Ensuite, il serait faux de croire que les auteurs de ces attentats – même fondamentalistes islamistes – ne sont pas en mesure de profiter des capacités de destruction et de perturbation offertes par les technologies modernes. En effet, il faut comprendre que l'archaïsme idéologique le plus extrême peut se concilier avec une certaine capacité à reprendre à leur compte les potentialités d'une société technologique occidentale que, pourtant, ils abhorrent idéologiquement. Cela a déjà été observé s'agissant de l'usage par ces mêmes mouvances islamistes des moyens audiovisuels (notamment télévisions par satellite) à des fins de propagande (16). Et ce ne serait pas la première fois que l'on constate cette relation ambivalente entre usage du progrès technique et adversaires de la société industrielle. Dans son très curieux « manifeste », le célèbre terroriste américain « Unabomber » (en réalité découvert depuis comme étant un ancien enseignant de mathématiques de Harvard, Theodore Kaczynski) n'hésitait ainsi pas à prôner la même réutilisation de la technologie moderne comme arme suprême de la « révolution » contre la société technique (17).

Enfin, il ne serait pas judicieux de tirer comme seule leçon de ces événements la nécessité d'accroître quantitativement la puissance de nos technologies de sécurité. Se prémunir contre la récupération de certaines fragilités des sociétés technologiques par un renforcement non réfléchi du caractère technologique de celles-ci ne serait assurément pas une attitude réfléchie. Remarquons en effet qu'une dérive vers le tout « techno-sécuritaire » serait quelque peu paradoxale alors que ces événements récents viennent justement de montrer le relatif échec des technologies de sécurité (18).

S'il doit y avoir réajustement de nos moyens collectifs de sécurité, c'est certainement à une réévaluation qualitative plus que seulement quantitative qu'il faudrait se prêter. Un déploiement inconsidéré de moyens techni-

(16) « *Les néo-traditionalistes ne méprisent pas la technique. Il nous est sans doute utile de savoir qu'ils sont technophiles, en ce sens qu'ils pensent que les nouvelles technologies de communication sont extrêmement bénéfiques pour la prédication* » (Sadok HAMMAMI, « L'exil des regards », *Les Cahiers de médiologie*, n° 3 (« Anciennes nations, nouveaux réseaux »), Gallimard, 1er semestre 1997, p. 189).

(17) « *La cause des révolutionnaires serait sans espoir s'ils s'attaquaient au système sans quelques moyens technologiques. Faute de mieux, ils devront utiliser les médias pour répandre leur message. Mais ils devront se servir de la technologie moderne dans un seul but : la lutte contre le système technologique* » (Unabomber [alias Theodore KACZYNSKI], *Manifeste : L'avenir de la société industrielle*, Éditions du Rocher, traduction française J.-M. Apostolidès, 1996, p. 179).

(18) Sur les illusions du « tout technologique » en matière de sécurité, et particulièrement en matière de sécurité de l'information (cryptographie, stéganographie, interceptions), *cf.* le point de vue de Franck LEPRÉVOST, professeur à l'Université Joseph Fourier de Grenoble, dans la *Revue Droit & Défense*, n° 1, 2002.

ques nouveaux créerait en effet, à terme, de nouvelles vulnérabilités : tout d'abord en conduisant la société à relâcher sa vigilance et à s'abandonner à l'illusion d'une sécurité parfaite; ensuite, en constituant des superstructures techniques (réseaux, centres de surveillance, bases de données, automatismes...) encore plus complexes à gérer et donc susceptibles d'engendrer – en cas de dysfonctionnement, de pénétration ou de contournement – encore plus de perturbations graves que cela est déjà possible aujourd'hui. Enfin, la généralisation des technologies sécuritaires (vidéosurveillance, traçabilité, interceptions...) dans la vie quotidienne ne conduirait qu'à faire de nos prétendues sociétés ouvertes et démocratiques des collectivités fermées et bloquées qui, en donnant l'impression de vivre dans une citadelle technologique assiégée, renforcerait l'impression d'exclusion du reste du monde qu'elles donnent déjà trop et qui est – pour une part – à la source de beaucoup de violences sociales et d'une partie du terrorisme.

Le débat autour des mesures anti-terroristes adoptées dans la suite immédiate des attentats de septembre (comme le Patriot Act américain, ou comme les amendements à la loi sur la sécurité quotidienne française [19]) doit donc aussi prendre en compte – au-delà des seuls aspects juridiques et de liberté publique – ce risque de voir s'accroître, par des mesures uniquement ou principalement techniques (notamment au niveau du contrôle des moyens de communication) la dérive technologique qui est justement à la source de la fragilité qu'ont exploitée les auteurs des terribles attentats du 11 septembre 2001.

(19) *Cf.* la chronique sur ces amendements : *Droit & Défense*, n° 4, 2001, pp. 45-47.