Questions de Recherche / Research in Question
N° 9 – Mai 2003

Le voleur et la matrice

Les enjeux du « cybernationalisme » et du « hacktivisme »

Laurent Gayer

Centre d'études et de recherches internationales
Sciences Po

LE VOLEUR ET LA MATRICE

Les enjeux du « cybernationalisme » et du « hacktivisme »

Laurent GAYER
Doctorant et enseignant à l'IEP de Paris

Résumé

Le cyberespace, dont l'internet constitue seulement l'une des composantes, ne se laisse pas réduire à un espace informationnel ou économique : c'est aussi un espace *politique*, qui mérite d'être analysé en tant que tel, à travers les mobilisations, les imaginaires et les pratiques de surveillance qu'il relaie. Plutôt qu'à une réflexion générale sur les « politiques mondiales de l'internet », cet article se consacre aux solidarités politiques transnationales qui se développent actuellement *sur* l'internet ou *grâce à lui*. Cette distinction est fondamentale, dans la mesure où le réseau des réseaux est à la fois le support de luttes sociales focalisées sur le monde « réel » et le foyer de nouvelles identifications et de nouveaux modes de protestation, qui se satisfont de leur virtualité. Les « réseaux revendicatifs transnationaux », dont l'origine remonte à la diffusion mondiale des mouvements abolitionniste et féministe, peuvent ainsi avoir recours à l'internet pour s'informer et communiquer ; leur usage des technologies de l'information demeure cependant assez banalement utilitaire et il n'apporte aucun bouleversement paradigmatique dans l'usage des médias par les groupes protestataires. L'essor du « hacktivisme » et du « cybernationalisme » apparaît bien plus novateur. Le « hacktivisme » désigne les usages du *hacking* (ici entendu comme piratage informatique) à des fins politiques. Il s'est développé au cours des années 1990, à la croisée de l'engagement politique, de l'activité ludique et de la performance artistique. Ses acteurs sont des groupes de *hackers* politisés ou des militants traditionnels fascinés par les nouvelles technologies de l'information et de la communication. L'avènement du « hacktivisme » témoigne ainsi de la rencontre entre deux univers jusqu'alors étrangers l'un à l'autre mais tous deux caractéristiques de la modernité tardive : l'« *underground* informatique » et les « nouveaux mouvements sociaux ». Le « cybernationalisme » désigne, pour sa part, l'utilisation intense et multiforme de l'internet par les entrepreneurs identitaires contemporains, qui trouvent appui sur le « réseau des réseaux » pour contourner les autorités étatiques qu'ils combattent et pour donner corps, par la parole et par l'image, aux communautés qu'ils (ré)inventent par-delà les frontières.

Abstract

Cyberspace, of which the Internet is a major but not the exclusive component, is more than an informational or an economic network : it is also a *political* space, which deserves to be analysed as such, through the collective mobilisations, the imaginary and the surveillance practices that it conveys. Rather than looking at the internet's world politics, this paper focuses on transnational political solidarities that are now emerging *on* and *through* the Internet. This differentiation suggests that the Internet is both the vector of social struggles focused on the "real" world, and the cradle of new identifications and new modes of protest that remain and will remain primarily virtual. Activists operating through transnational "advocacy networks" may use the Internet to receive or spread information, but their use of the Information Technologies (IT) remains purely instrumental and does not imply any paradigmatic shift in the tactical uses of the media by protest groups. "Hacktivism" and "cybernationalism" appear far more promising, as far as the invention of new repertoires of collective action is concerned. "Hacktivism", which refers to the use of hacking techniques for political ends, emerged during the 1990s, at the crossroads between activism, play and art. The emergence of "hacktivism" was made possible by the meeting of two social actors that epitomize our late modernity : new social movements and the "digital underground". "Cybernationalism", for its part, was given shape in the last decade by ethnic entrepreneurs who rely on the IT to challenge the political authorities of their home states and to materialise, through words and images, the communities they are (re)inventing beyond borders.

> Case avait vingt-quatre ans. A vingt-deux, il était un *cow-boy*, un braqueur, l'un des tous bons de Zone. (…) Il avait opéré en trip d'adrénaline pratiquement permanent, un sous-produit de la jeunesse et de la compétence, branché sur une platine de cyberspace maison qui projetait sa conscience désincarnée au sein de l'hallucination consensuelle qu'était la matrice. Voleur, il avait travaillé pour d'autres voleurs plus riches, des employeurs qui lui fourguaient le logiciel bien particulier requis pour pénétrer les murs brillants des réseaux de grosses sociétés, pour tailler des ouvertures dans de riches champs de données.
>
> William Gibson, *Neuromancien*.

Inventeur du terme « *cyberspace* », l'auteur de science-fiction américain William Gibson mérite d'être (re)lu à l'aune des développements contemporains de la Toile mondiale (GIBSON, 1984 ; 1986 ; 1988). Ses romans anticipent l'essor d'un réseau informatique mondial (la « *matrice* ») dont les firmes multinationales, les appareils sécuritaires de la planète et leurs employés souvent rebelles se disputent le contrôle. Case, le héros de *Neuromancien*, est l'un d'entre eux. Jeune et brillant informaticien, il est aussi un « *cow-boy* » et un « braqueur », ce qui le rend parfois difficilement contrôlable pour ses employeurs haut placés. Baignant dans une atmosphère cosmopolite, entre bars interlopes tokyoïtes et visites à Topkapi, l'œuvre de Gibson a profondément marqué les pionniers de l'internet. Pour Allucquere Rosanne Stone, « l'importance critique du livre de Gibson [*Neuromancien*] s'explique par la façon dont il a enclenché une révolution conceptuelle parmi les travailleurs dispersés qui travaillaient dans le domaine de la réalité virtuelle depuis des années. (…) L'existence du roman de Gibson et l'imaginaire social et technologique qu'il articulait permit aux chercheurs travaillant dans le domaine de la réalité virtuelle – ou, sous sa nouvelle dénomination, du cyberespace – de se reconnaître et de s'organiser en tant que communauté » (STONE, 1992, cité par HILLIS, 1996 : 87). En plaçant notre réflexion sous le signe de Gibson, il ne s'agit donc pas de s'aventurer sur le terrain de la critique littéraire ou des *cultural studies*, mais de mettre les formes de résistance « populaire », aujourd'hui véhiculées par l'internet, en relation avec l'imaginaire des individus et des groupes qui les animent. Le caractère proprement « populaire » de ces nouvelles formes de mobilisation politique est néanmoins sujet à caution. Le capital social et technologique indispensable aux activités de programmation et de piratage (*hacking*) sur l'internet paraît en effet les réserver à une poignée d'initiés de par le monde, même si les *hackers* revendiquent souvent leur « basse extraction technologique » en se présentant comme des bricoleurs partis de rien ou presque : trois bouts de fil électrique et une console Amiga ou Atari.

Apparu sur les campus du MIT et de Berkeley au début des années 1960 (LEVY, 1984 ; RAYMOND, 2001 : 1-18), le terme « *hacking* » est dès son origine ambivalent, puisqu'il suggère à la fois l'idée de « promenade » et d'« abattage ». Depuis les années 1980, les médias lui ont donné une connotation résolument criminelle et les *hackers* légalistes s'identifient désormais comme « *white hats* », par opposition aux « *black hats* » ou « *crackers* ». Depuis quelques années, on assiste également à la multiplication des « *script kiddies* », ou « *script monkeys* », ces jeunes pirates en herbe qui font usage de programmes clés en main pour « hacker » les ordinateurs. Plus récemment encore, on a assisté à l'émergence du « hacktivisme », qui désigne l'utilisation des nouvelles technologies et du *hacking* (entendu ici comme piratage informatique) à des fins sociales ou politiques.

C'est à ces pratiques contestataires innovantes que nous souhaitons nous intéresser ici, en écho à la question de Gilles Deleuze : « quand les forces de l'homme se composent avec celles du silicium, qu'est-ce qui se passe, et quelles nouvelles formes sont-elles en train de naître ? » (DELEUZE, 1990 : 137). Afin d'apporter un début de réponse à cette question, nous chercherons ici à éclairer l'articulation entre opérations disciplinaires et pratiques contestataires dans le cyberespace, en envisageant ce dernier comme une arène de mobilisation prolongeant le réel et ses rapports de force plutôt qu'instituant une « réalité virtuelle », comme le suggère l'oxymore actuellement en vogue. Ancrant notre étude dans une réflexion sur les formes du contre-pouvoir informatique, nous rejoindrons également les interrogations des théoriciens du nationalisme et des « anthropologues de la modernité » (BERTRAND, 2000) sur l'articulation entre mondialisation et processus d'identification. De fait, la question de la « résistance internet » englobe celles du « hacktivisme » et du « cybernationalisme ». Le premier peut être défini comme l'usage des techniques de *hacking* à des fins politiques et le second comme l'utilisation intense et multiforme de l'internet par les entrepreneurs identitaires contemporains, à des fins de médiatisation, de communication, de financement et parfois d'imitation de l'Etat. Les « cybernationalistes » trouvent ainsi appui sur l'internet pour contourner les autorités étatiques qu'ils combattent et pour donner corps, par la parole et par l'image, à la communauté qu'ils (ré)imaginent par-delà les frontières. Si le développement du « capitalisme de l'imprimé » a joué un rôle décisif dans la construction des identités nationales à partir du XVIIIe siècle, dans les colonies puis dans les métropoles elles-mêmes (ANDERSON, 1983), le développement du « capitalisme de l'hypertextualité » s'accompagne quant à lui de la production discursive de « cybernationalités » déterritorialisées, ancrées à un foyer originel mais en mouvement perpétuel, nouveaux peuples nomades qui trouvent dans le virtuel un support à leurs identités imaginées dans un réel mouvant.

Plutôt qu'il ne témoigne d'une résurgence des particularismes en *réaction* à la diffusion de normes et d'une économie mondiales, le « retour du local » (VIARD, 1994) que l'on observe depuis quelques années s'opère en réalité en relation à la mondialisation des économies et des idées. Le « néo-localisme » (CLARKE & GOETZ, 1993) reposerait ainsi sur l'articulation entre réticularisation du monde sous l'influence des réseaux transnationaux et transformation des modes de subjectivation individuels et collectifs, auxquelles participe directement l'essor d'internet. Nous insisterons donc ici sur l'interaction entre mondialisation et « nouvelles ethnicités » (HALL, 1992), en nous démarquant clairement des thèses sur le « clash des spatialisations » (BARBER, 1996). Notre approche se refusera alors à envisager la « mondialisation » et l'« ethnicité » comme des antonymes. Au contraire, elle se propose de les réconcilier pour s'intéresser aux échanges à double-sens qui s'établissent entre eux. Roland Robertson note ainsi que « la promotion de la localité est souvent assurée par le bas ou du dehors. Une large part de ce que l'on reconnaît comme local est en fait le local exprimé en termes de recettes générales de la localité » (ROBERTSON, 1995 : 26). Ces identifications « transversales »[1], au carrefour du local et du global, rétroagissent sur l'espace mondial en s'accompagnant de « diplomaties identitaires » qui s'adressent aux Etats, aux organisations intergouvernementales, aux institutions supranationales et enfin aux « réseaux revendicatifs transnationaux » (*advocacy networks*) (KECK, SIKKINK, 1998). L'internet joue ici un rôle décisif, puisqu'il constitue la principale interface entre *influences* et *incidences* transnationales des politiques « nationalitaires » contemporaines, au fort potentiel déstabilisateur. Rappelons que l'épithète « nationalitaire » désignait essentiellement, dans les années 1970, les régionalismes de gauche mêlant critiques de l'Etat-nation et du capitalisme. Alain Dieckhoff a cependant récemment proposé d'étendre le terme aux « nationalismes de dissociation », par opposition aux « nationalismes centralistes ». Le caractère « déstabilisateur » des mouvements nationalitaires n'implique pas nécessairement un potentiel « désintégrateur » : ils peuvent chercher à remodeler – souvent violemment – la carte mondiale mais ils y parviennent en fait rarement et, loin d'apparaître comme des forces opposées à la mondialisation, ces mouvements en procèdent autant qu'ils y contribuent (DIECKHOFF, 2000).

Instrument de communication, de médiatisation, de transaction et de contestation mais aussi de surveillance, l'internet constitue à la fois un outil et un espace de (contre-) pouvoir, ce qui rend particulièrement complexe toute tentative d'analyse de ses enjeux politiques. Plutôt qu'à une réflexion globale sur ces derniers, il s'agira donc ici de nous

[1] Cette notion s'inspire des « politiques transversales » de James Rosenau (ROSENAU, 1997 : 5). Sur la notion de « transversalité » en relations internationales, on pourra également se référer à SOGUK & WHITEHALL, 1999.

concentrer sur un sujet déjà vaste : les « stratégies du désordre »[2] qui se déploient actuellement *sur* et surtout *grâce* au *world wide web*. Cette distinction est fondamentale puisqu'elle implique que certaines mobilisations « hacktivistes » et « cybernationalistes » se satisfont de leur virtualité alors que d'autres prolongent l'action de mouvements contestataires encore focalisés sur le monde « réel ».

CYBERPOLIS : POUR UNE SOCIOLOGIE POLITIQUE DE LA CONTESTATION DANS LE CYBERESPACE

Les « politiques de l'internet » rencontrent depuis quelques années un engouement certain auprès des sociologues et des politologues. Nombre de travaux consacrés aux usages et aux enjeux politiques d'internet se trouvent malheureusement desservis par leur caractère utopique, dans la mesure où ils voient, dans le « réseau des réseaux », le nouveau centre névralgique du social et du politique, ainsi qu'un nouvel instrument d'émancipation des masses menant à la « cyberdémocratie » directe. Pour échapper à ces antiennes sur le monde enchanté ou, au contraire, fragmenté et atone, que nous promettrait l'essor du cyberespace, nous avons choisi de privilégier ici les usages contestataires de l'internet propres à deux grands types d'acteurs : les « hacktivistes » et les « cybernationalistes ». Avant de nous intéresser directement aux pratiques de « cyber-résistance », il nous faudra rappeler les origines et les enjeux sociologiques du *hack*, matrice des usages contestataires de l'internet qui témoigne d'une maîtrise de la *mètis*, c'est-à-dire d'une intelligence rusée qui ne sépare pas conception et usage (DETIENNE & VERNANT, 1974).

L'appropriation des techniques de *hacking* ou de l'esprit bricoleur et provocateur des premiers *hackers* par les « hacktivistes » et les « cybernationalistes » contemporains s'est accompagnée d'une politisation du *hacking* et de ses représentations par les pouvoirs publics, au point que la Grande-Bretagne reconnaît, depuis 2000, le piratage informatique comme une forme de terrorisme. La rencontre du monde de l'« *underground* numérique » et des milieux militants traditionnels s'est opérée dans la seconde moitié des années 1990 et

[2] Nous empruntons ce concept à Bertrand Badie, qui l'a développé à l'occasion de son enseignement de relations internationales à l'IEP de Paris. Les « stratégies du désordre » désignent les politiques belligènes asymétriques d'acteurs affrontant des adversaires plus puissants qu'eux et se sachant par là même voués à l'échec, mais ne craignant pas de s'y ruer, par bravade ou par désir de martyre.

leur rapprochement se poursuit actuellement, non sans heurts. Les différends qui ont pu éclater entre *hackers* et hacktivistes ou cybernationalistes suggèrent que l'univers de la contestation en ligne est profondément bariolé, parcouru de nombreux clivages internes. Comment, alors, approcher ces « p@rtisans » et leurs adversaires, tant empiriquement que théoriquement ? Comment découvrir leurs modes opératoires et leur discours, et quels problèmes spécifiques de traitement et d'interprétation posent-ils ? Ces questions nous amèneront à nous interroger sur la nature spécifique du *medium* internet, à la fois espace et outil de communication, de consommation, de protestation et de surveillance, reposant sur le principe de l'émetteur-récepteur, ou encore du « *many to many* », par opposition aux médias audiovisuels, qui reposent sur le principe du « *few to many* » (TRAUTMANN, 2000 : 4). Ce sont ces caractéristiques du cyberespace qui constituent le contexte socio-technique dans lequel les hacktivistes et les cybernationalistes opèrent, qui expliquent largement la spécificité des formes de contestation « virtuelles » par rapport à leurs contreparties « réelles », la distinction entre ces deux domaines de l'expérience perdant aujourd'hui de sa force heuristique, si tant est qu'elle en ait jamais eu.

Le hacking, un usage (ré)créatif des technologies de l'information et de la communication

Dans son travail pionnier sur « l'internet militant », Fabien Granjon suggère que l'étude des usages contestataires des nouvelles technologies de communication pose fondamentalement le problème de « la médiation réciproque des objets techniques et des pratiques sociales » (GRANJON 2001 : 7). Ce questionnement renouvelle les interrogations des sociologues de la communication, qui insistent sur la « genèse continue de l'individualité de l'objet technique » et sur la manière dont celui-ci contribue à la « prise de forme des activités et des relations sociales qu'il médiatise » (QUERE, 1992 : 45). Cette problématique de la médiation réciproque des techniques de communication et des pratiques sociales a notamment été développée par la sociologie des usages, qui s'est imposée dès les années 1960 dans la recherche empirique anglo-saxonne et qui suggère de regarder non plus seulement « ce que les médias font aux individus » mais également « ce que les individus font des médias » (JOUET, 2000 : 493). La sociologie des usages française, inspirée par les travaux de Michel de Certeau (CERTEAU, 1990), invite quant à elle à dévoiler la manière dont les usagers, véritables « participants actifs » plutôt que simples consommateurs, s'approprient les médias, éventuellement en les détournant de leurs fonctions initiales. La

programmation informatique amateur et le piratage, qui constituent les deux faces du *hacking*, apparaissent comme des cas emblématiques d'appropriation des technologies numériques. L'« appropriation » constitue le pôle opposé de l'« adoption » sur le *continuum* des usages d'un objet technique ; elle demande maîtrise technique et cognitive de cet objet, s'intègre aux pratiques quotidiennes de l'usager et « ouvre vers des possibilités de détournements, de contournements, de réinventions ou même de participation directe des usagers à la conception des innovations » (BRETON & PROULX, 2002 : 255-256).

Le terme « *hack* » est apparu dans les années 1950 parmi les informaticiens du MIT pour désigner un raccourci de programmation, le plus fameux de ces *hacks* « préhistoriques » étant sans aucun doute celui qui, en 1969, conduisit deux employés de Bell Lab, Dennis Ritchie et Ken Thompson, à mettre au point le système d'exploitation UNIX. Deux ans plus tard, un vétéran de la guerre du Vietnam, John Draper, découvrit que la fréquence émise par les sifflets accompagnant les paquets de céréale Cap'n Crunch (2600 Mhz) correspondait à celle d'une pièce de 25 cents tombant dans la fente d'un téléphone public américain. Le *phreaking*, c'est-à-dire l'usage illégal des réseaux téléphoniques, était né ; il constitue depuis lors une variété de *hacking* spécifique, avec ses publications (l'*International Youth Party Line Newsletter*, devenue le *Technical Assistance Program*), ses clubs d'afficionados et ses figures légendaires. Dans les années 1980, une « scène » *hacker* émergea aux Etats-Unis, en Europe et en Australie, autour de ces passionnés du téléphone et des ordinateurs, qui commencèrent à connecter leurs machines par le biais des lignes téléphoniques, donnant naissance aux BBS (*Bulletin Board Systems*). Ceux-ci furent bientôt reliés par le réseau Fidonet, qui selon son fondateur « reposait explicitement sur des principes sociaux anarchistes » (cité par FLICHY, 2001 : 58-59). Loin de former une « communauté » homogène, ces usagers compulsifs et inventifs des technologies de l'information et de la communication (TIC) étaient affiliés à divers « clans » qui se livraient parfois des combats sans merci dans le cyberespace. En 1990, les membres de la Legion of Doom (LoD), un groupe de *hackers* américains fondé par Eric Bloodaxe (alias Chris Goggans) en 1984, affrontèrent ainsi les Masters of Deception (MoD), emmenés par un dissident de la LoD connu sous le pseudonyme de « Phiber Optik » (Mark Abene de son vrai nom). Le conflit finit par attirer l'attention du FBI et l'affaire se termina par l'arrestation de Mark Abene et de ses acolytes, signant la fin d'une époque. En 1986, le Congrès américain adopta le Federal Computer Fraud and Abuse Act, dont Robert Moris, le jeune programmeur à l'origine du premier « vers » informatique, fut le premier à faire les frais en 1988, écopant de 10 000 dollars d'amende et d'une peine de travail d'intérêt général pour avoir conduit à la destruction de 6 000 ordinateurs connectés à internet. La même année, Kevin Mitnick, surnommé le « *lost boy of cyberspace* » par les médias américains, pénétra illégalement

dans le système informatique de Digital Equipment Corporation, il fut condamné à un an de prison. En 1995, Mitnick fut à nouveau emprisonné pour avoir piraté les réseaux téléphoniques américains et dérobé 20 000 numéros de cartes de crédit. Il fut arrêté après une rocambolesque course-poursuite contre sa Némésis, le *hacker* renégat Tsutomu Shimamura (HAFNER & MARKOFF, 1991). Cet épisode resté célèbre suggère que, pour déjouer les tours des *hackers*, les gouvernements n'ont eu d'autre recours que de « retourner » certains d'entre eux, rappelant que Mètis ne peut être vaincue que par ses propres armes : la ruse, la tromperie et la surprise (DETIENNE & VERNANT, 1974 : 112). Outre certains services de police et de renseignement, comme le FBI et la NSA aux Etats-Unis ou la DST en France (GUISNEL, 1995), des entreprises telles qu'IBM ont également engagé des *hackers* pour se prémunir des attaques électroniques. En cas d'intrusion illégale, l'équipe de *hackers* mercenaires cherche à neutraliser l'intrus en anticipant ses mouvements et en guettant le moindre relâchement de vigilance de sa part pour le surprendre. Ces protections sont devenues d'autant plus nécessaires que les actes de piratage se sont multipliés avec l'essor du *world wide web*, une série d'attaques spectaculaires contre les plus grands sites de commerce en ligne, en février 2000, ayant frappé les esprits, suivie quelques mois plus tard de l'apparition du virus « *I love you* ». Le *hacking,* qui désignait à l'origine les usages « rusés » du téléphone et des ordinateurs, en est ainsi venu à désigner, dans le langage courant, ce que les *hackers* qualifient eux-mêmes de « *cracking* », c'est-à-dire l'intrusion illégale dans les systèmes d'information. Celle-ci est tolérée par l'orthopraxie *hacker*, « tant que le *cracker* ne se livre à aucun acte de vol, de vandalisme ou d'atteinte à la vie privée »[3], mais également tant que ces actes ne portent pas atteinte à la libre circulation de l'information sur les réseaux. Dans le cas contraire, le *cracker* devient un « *black hat* » et se trouve mis au ban de la « scène ». Nous verrons que le conflit entre *hackers* et « hacktivistes » trouve ici ses origines, les premiers accusant les seconds de violer la *hacker ethic*[4] en se livrant à des opérations de déni d'accès ou de défiguration de certains sites internet.

Les appropriations du téléphone et des ordinateurs auxquelles se livrent les *hackers* sont filles de *mètis*, l'intelligence rusée du *trickster*, du pêcheur et du navigateur, qui règnent sur un monde fuyant en se coulant dans son flot, en se faisant eux-mêmes flux (DETIENNE

[3] Cf., sur ce point, les *jargon files*, monuments de la cyberculture régulièrement réactualisés par ses usagers depuis les années 1970 : http://info.astrian.net/jargon/terms/h/hacker_ethic.html.

[4] Cette éthique repose sur les six points suivants : (1) « l'accès aux ordinateurs devrait être total et sans limite » ; (2) « toute information devrait être libre » ; (3) « il convient de se défier de l'autorité et de promouvoir la décentralisation » ; (4) « les *hackers* devraient être jugés sur leur production et non sur de faux critères comme les diplômes, l'âge, la race ou la situation sociale » ; (5) « vous pouvez créer de l'art et de la beauté avec un ordinateur » ; (6) « les ordinateurs peuvent transformer votre vie, pour le meilleur. » (LEVY, 1984 : 40-45 ; nous utilisons ici la traduction de FLICHY, 2001 : 85)

& VERNANT, 1974). Le terrain de jeu des *hackers* est un « espace navigable » (le cyberespace), un « réseau » qui est aussi un « filet » (le *net*), ou encore une toile d'araignée (le *web*). Dans cet environnement fluctuant, parsemé de pièges, le talent d'un *hacker* ne se résume pas à son expertise technique ; il se reconnaît essentiellement à sa capacité à *prévoir*, à ajuster son action aux possibles, au stade de la conception puis de l'usage. De fait, pour l'individu doté de *mètis*, il n'existe pas de hiatus entre construire et conduire : « parce qu'ils sont étroitement solidaires de l'intelligence technicienne d'Athéna, le navire et le char apparaissent comme des instruments agis autant que fabriqués. » (*ibid* : 230) Il en va de même pour les outils informatiques conçus puis utilisés par les *hackers*, sur le modèle néo-platonicien de l'*open-source*, en vertu duquel un programmeur développe un système ou un logiciel novateur et le propose gratuitement pour utilisation et *amélioration* sur un réseau donné. Ces systèmes d' « intelligence collective » (HILTZ & TUROFF, 1978), ressuscitant le principe de la *synusia* platonicienne (HIMANEN, 2001), s'appuyaient hier sur l'Altair 8800, un micro-ordinateur qu'il fallait construire soi-même et qui familiarisait ainsi aux principes de base du *hacking* avant même que l'on puisse en faire usage (LEVY, 1985). Les *hackers* contemporains s'appuient quant à eux sur Linux, système d'exploitation alternatif à Windows initialement développé par le *hacker* finlandais Linus Torvalds mais perpétuellement amélioré par ses usagers (BLONDEAU, 1999 ; MOODY, 2002). Le mouvement transnational pour l'*open source*, emmené par le « cyber-gourou » Richard Stallman, constitue le dernier avatar en date de ces « communautés épistémiques » (HAAS, 1992) qui ont donné naissance à l'internet (FLICHY, 1999) et au sein desquelles la frontière entre conception et utilisation des objets techniques apparaît floue, au point que la notion de « *copyright* » s'y efface au profit de celle de « *copyleft* », la production individuelle n'étant plus valorisée qu'au titre de fragment d'un patrimoine technique et cognitif commun (DIBONA, 1999 ; PAVLICEK, 2000).

Si le *hacking* apparaît comme une manifestation de la *mètis*, que maîtrisaient si bien le pêcheur, le navigateur ou l'aurige grecs, il s'agit également de resituer ces pratiques dans l'histoire du piratage médiatique. Les premiers *hackers* se comparaient souvent aux radioamateurs et partageaient avec eux un double projet : « communiquer entre eux et réaliser des performances techniques analogues à celles des professionnels » (FLICHY, 2000 : 255). Le *hacking* est ainsi à l'informatique ce que les premières radios libres furent à la radiophonie : un usage imprévu et (ré)créatif, flirtant avec l'illégalité. Dans les années 1960, les *disc-jockeys* de *Radio Caroline*, diffusant à partir d'un vieux cargo, changèrent à jamais le paysage radiophonique britannique, contraignant la BBC à créer une chaîne spécialement consacrée à la musique pop, *Radio 1* (CAZENAVE, 1980 : 40 ; CHAPMAN, 1992). En 1976, les expérimentations de Steve Wozniak au sein du Homebrew Computer

Club, un groupe de *hackers* de San Francisco, conduisirent quant à elles à la mise au point du premier *personal computer* (PC), l'Apple II (LEVY 1984 : 244-267). Cette révolution fut décisive dans l'histoire de l'informatique. On peut se rappeler qu'en 1943, Thomas Watson, président d'IBM, déclarait : « je pense qu'il y a un marché mondial pour environ cinq ordinateurs » ; en 1977, Ken Olsen, cofondateur et président de Digital Equipment Corporation, affirmait quant à lui : « il n'y a aucune raison que les gens veuillent un ordinateur chez eux ».

Si, à la différence des *hackers*, les animateurs de radios libres étaient le plus souvent politisés, ces deux groupes se rejoignent dans la passion qui les relie à leur média de prédilection et dans leur désir d'expérimenter de nouveaux usages de celui-ci. Le *hack*, qui dans les années 1970 en est venu à désigner l'intrusion illégale dans un système informatique, doit remplir trois conditions pour mériter la considération de la « scène » : il doit être simple, illicite, et témoigner d'un savoir-faire hors du commun (TURKLE, 1984 : 232). Comme l'explique « Ralph », un *phreaker* néerlandais, interviewé par Tim Jordan et Paul Taylor, « [un bon *hack*] dépend de la manière dont on l'accomplit ; il y a ces gars qui pensent à des trucs, qui envisagent les divers composantes d'un combiné téléphonique, et ils se disent 'attends une minute, si j'essaie ça, ça pourrait marcher', et alors ils essaient [*so they experiment*], ils coupent le fil, et ça marche ; c'est là qu'ils deviennent des *hackers* » (JORDAN & TAYLOR, 1998 : 759). Le *hacker* n'est donc pas nécessairement un pirate informatique : c'est avant tout un bricoleur en quête d'usages alternatifs de sa technologie de prédilection, qu'il s'agisse du téléphone, dans le cas des *phreakers*, ou des ordinateurs, dans le cas des *hackers* proprement dits. Cette quête est fondamentalement ludique, comme l'explique Linus Torvalds, concepteur du système d'exploitation *open source* Linux : « pour le *hacker* […] l'ordinateur est en lui-même une source d'amusement [*entertainment*] »[5]. Pekka Himanen renchérit, dans le même ouvrage, en suggérant que « le *hacker* programme parce qu'il trouve la programmation intrinsèquement intéressante, excitante et joyeuse » (HIMANEN, 2001 : 3). On retrouve donc chez les *hackers* certains traits communs à tous les pirates médiatiques : une passion pour la technologie et pour ses usages expérimentaux et transgressifs, souvent assortie d'un esprit fantaisiste. Cette fantaisie se manifeste aussi bien dans les opérations et les avatars (identités numériques) de nombreux *hackers* que dans leurs actes quotidiens. Ainsi, Sandy Lerner, à l'origine des « *routers* » sur internet, est-elle célèbre pour ses promenades équestres dénudées, alors que Richard Stallman, le « pape » de l'*open source*, exorcise, au cours de séances mouvementées, les ordinateurs de ses disciples, éloignant à jamais d'eux les logiciels commerciaux. Eric Raymond, un des ténors

[5] Il n'est donc pas anodin que le récit autobiographique de Torvalds sur la naissance de Linux soit intitulé *Just for Fun* (TORVALDS, DIAMOND, 2001).

de la « cyberculture », est pour sa part un passionné de jeux de rôles, et on l'a souvent surpris à rôder dans les bois de sa Pennsylvanie natale déguisé en chevalier ou en sénateur romain (*ibid* : 5). Agé de 24 ans lorsqu'il inventa le premier ordinateur personnel, Steve Wozniak, qui « ressemblait à un clochard », avec ses cheveux gras tombant sur ses épaules et sa barbe mal taillée, animait quant à lui de son domicile un service appelé « *dial-a-joke* », qui donnait accès à une série interminable de plaisanteries « polonaises » (l'équivalent de nos « blagues belges »). Wozniak était également un passionné de jeux électroniques et de tennis, sport dans lequel il excellait du fait de ses remarquables effets liftés. Il n'est donc pas étonnant que l'Apple II, le premier ordinateur personnel de l'histoire, qu'il mit au point avec son ami Steve Jobs, fut avant tout « le genre d'ordinateur avec lequel il avait envie de jouer » (LEVY, 1984 : 244-246).

La « scène » *hacker* est une « communauté épistémique » (HAAS, 1992) fondée sur l'échange et l'émulation, mais également une « communauté de joueurs » (*play-community*) qui s'entoure du secret pour se doter d'une identité propre et qui continue d'exercer son influence sur ses membres lorsque le jeu s'est, temporairement, interrompu (HUIZINGA, 1950). A l'instar des communautés nationales, la « scène » est naturellement une communauté imaginée parce qu'aucun de ses membres ne parviendra jamais à connaître tous les autres. A cette dimension *imaginée* de la « scène » s'ajoute son caractère partiellement *imaginaire*, du fait du jeu de masques auquel se livrent les *hackers* en et hors ligne, par le biais du pseudonyme et du déguisement, le pouvoir de métamorphose étant lui aussi un attribut de Mètis (DETIENNE & VERNANT, 1974 : 28).

Les *hackers* se rapprochent également des pirates radiophoniques de par leur contestation des monopoles ou des oligopoles publics et privés sur leur média de prédilection. Par-delà ses divisions, la scène *hacker* se trouve unie par son hostilité envers les multinationales informatiques et ses membres déploient des trésors d'ingéniosité technique pour mettre au point de nouveaux programmes d'exploitation ou de nouveaux logiciels concurrençant ceux de Microsoft. En cela, ils sont bien des *tricksters*, affrontant les puissants par des moyens détournés, préférant la ruse au choc frontal ; le Décepteur est en effet « un héros mal identifiable, divin par certains aspects, toujours errant, ignorant les limites du bien et du mal, puissamment sexué, engagé dans des aventures caractérisées par l'astuce et la tromperie » (BALANDIER, 1992 : 45). La programmation, pour les *hackers*, est d'abord une affaire de *tricks*, un jeu auquel ils s'adonnent en réseau ou en solitaire, livrant un combat contre leurs adversaires mais aussi et surtout contre la machine et, au final, contre eux-mêmes. Le *hack* est donc un moment de subjectivation intense puisqu'il conduit le

hacker à se redécouvrir en se positionnant par rapport aux autres, au cours d'une expérience qui le conduit aux frontières de la légalité, et parfois au-delà.

L'informatique encourage de tels usages (ré)créatifs imprévus car elle est fondée sur un principe d'interactivité qui lui est propre. A la différence de l'auditeur ou du téléspectateur, l'usager d'un ordinateur équipé d'un modem est à la fois récepteur et émetteur, et la polyvalence de cet outil est supérieure à celle de tous les autres médias, au point que « c'est l'utilisateur qui construit le produit final avec ses propres 'inputs' » (JOUET, 1997 : 300). Cette plasticité des usages de l'informatique favorise la construction et la manifestation de la subjectivité, dans la mesure où les usagers s'approprient les attributs de la machine pour la mettre au service de leur désir (TURKLE, 1984). La programmation personnelle, sur laquelle s'appuie le *hacking*, témoignerait ainsi d'une « communication subjective avec la machine », où l'informaticien amateur cherche à rivaliser avec l'intelligence de l'ordinateur pour s'affirmer et se situer par rapport aux autres (JOUET, 1997 : 300). Cette quête d'accomplissement personnel n'a rien de remarquable en soi et, comme le remarque Fabien Granjon, « la figure de l'usager actif, *entrepreneur de sa propre vie* devient une référence prépondérante qui n'est pas sans rappeler l'un des modes d'action privilégiés à partir duquel s'organise les nouvelles formes d'engagement militant, à savoir un détachement des appartenances collectives traditionnelles au profit de la performance individuelle » (GRANJON, 2001 : 11). En se réalisant au moins partiellement dans le cyberespace, ces nouvelles formes de protestation posent cependant des problèmes spécifiques.

Eléments de géographie politique du cyberespace

Emprunté à la science-fiction, le terme « cyberespace » demande à être explicité pour se prêter à un usage scientifique. Les nouvelles technologies de l'information et de la communication dessinent-elles ainsi un véritable espace ou opèrent-elles au contraire dans un non-lieu virtuel ? Etymologiquement, le cyberespace est un « espace navigable », sans contours précis. Morphologiquement, celui-ci ne se laisse pas réduire à un lieu ou à une technologie donnés, mais coagule dans un espace conceptuel « une myriade de cyberespaces en expansion rapide, chacun permettant une forme spécifique d'interaction et de communication digitales » (DODGE & KITCHIN, 2001 : 1). Il s'agit notamment des réseaux de communication traditionnels (téléphone/fax), des technologies liées à la « réalité

virtuelle »[6] et de l'internet, ces trois éléments constitutifs du cyberespace convergeant actuellement à travers de nouveaux supports. Ainsi que le suggèrent les premiers travaux de géographie politique consacrés à ce nouvel objet d'étude, le cyberespace est fondamentalement un espace d'action et de communication complétant les espaces géographiques traditionnels plutôt que s'y substituant ou opérant de manière autonome par rapport à eux. Sa nature réticulée implique cependant que, « dans ce cas, l'espace n'est pas géométrique mais relationnel, dans la mesure où il se trouve composé par des flux » (FROEHLING, 1997 : 293). Cette nature réticulée du cyberespace permet aux individus et aux organisations « d'opérer avec plus de flexibilité par rapport aux logiques géographiques tangibles [*real-space geographies*] » (DODGE & KITCHIN, 2001 : 15), sans pour autant s'en détacher complètement.

Espace conceptuel, le cyberespace est également un espace *virtuel*, c'est-à-dire une « représentation, perception ou construction d'un espace dans lequel les sujets et les objets établissent des relations sans y être présents simultanément » (GUILLAUME, 2000 : 61). L'avènement de tels espaces virtuels a précédé celui de l'internet et les transformations de l'édition et des techniques de lecture survenues au XVIIIe siècle, puis le développement du télégraphe et du téléphone au XIXe et enfin l'apparition de la radio, du cinéma et de la télévision au XXe, se sont accompagnés de la démocratisation de la virtualité, les médias de masse ayant engendré « un nouveau monde a-spatial mêlant étroitement l'illusion et le réel, provoquant les effets d'ubiquité dont les hommes avaient rêvé depuis longtemps » (*ibid* : 65).

Il est courant d'exagérer la portée sociale des innovations technologiques et l'engouement actuel des sociologues et des politologues pour l'internet ne doit pas nous faire oublier que la rencontre entre l'internet des universitaires et le *net* des *hackers*, qui a donné naissance au *world wide web* dans les années 1990, ne fut qu'une nouvelle étape du processus historique de réticularisation du monde, amorcé par l'invention des techniques d'impression et poursuivi par la diffusion des médias électriques puis électroniques. Les discours utopiques entourant actuellement l'internet ne doivent pas nous dissimuler la généalogie de la virtualité et de son corollaire, « l'utopie planétaire » (MATTELART, 2000). Loin de conduire à l'isolement d'individus toujours plus anomiques, l'essor du virtuel s'est en effet accompagné d'imaginaires de la globalité et de relations sociales transnationales toujours plus denses. Il s'agit ainsi de se rappeler des propos du ministre français aux

[6] Dès 1965, un étudiant du MIT, Ivan Sutherland réfléchit, dans un article intitulé « The ultimate display », à un espace informatique en trois dimensions (3 D) dans lequel il serait possible de s'immerger pleinement. Dans les années 1970, Sutherland mit au point un environnement de réalité virtuelle à l'aide d'une lourde machine posée sur la tête de l'usager. Il fallut pourtant attendre les travaux de la NASA, dans les années 1980, pour que ces

Affaires étrangères, M. Drouyn de Lhuys, accueillant le 13 avril 1865 les délégués d'une vingtaine de nations européennes venus se réunir à Paris pour poser les jalons d'une Union télégraphique internationale. Pour lui, le télégraphe était « ce prodigieux engin de transmission, ce fil électrique, sur lequel la pensée, comme emportée par la foudre, vole à travers l'espace et qui permet d'établir un dialogue rapide, incessant, entre les membres dispersés de la famille humaine » (cité dans *ibid* : 164). La même année, un réseau de câbles télégraphiques sous-marin fut construit à travers le monde et trois ans plus tard, en 1868, Louis Figuier pouvait écrire : « Maintenant, plusieurs contrées, séparées par la mer sur une distance considérable, sont en relation électrique continue, et correspondent de manière instantanée, comme si elles n'étaient séparées que par un intervalle de quelques lieues » (cité par GUILLAUME, 2000 : 65). Le développement de la radiophonie s'accompagna lui aussi de cette « rhétorique du sublime technologique » qu'évoque Léo Marx dans ses pages sur la machine à vapeur (MARX, 1964, cité par FLICHY, 2000 : 260). Dans une nouvelle écrite en 1912, Francis Collins prophétise ainsi l'apparition d'une gigantesque toile communicationnelle mondiale : « Imaginez une gigantesque toile d'araignée avec de multiples fils partant dans toutes les directions depuis New York jusqu'à des terres ou des mers situées à des milliers de milles. Dans sa station, notre opérateur peut être comparé à une araignée constamment éveillée surveillant le plus faible tremblement dans le coin le plus éloigné de son invisible fabrique. Les différents opérateurs éloignés discutent et plaisantent les uns avec les autres comme s'ils étaient dans la même pièce » (cité par DOUGLAS, 1987 : 199). Le développement du *net* a alimenté des imaginaires de la communication assez similaires (FLICHY, 2001), la « toile d'araignée » de Collins se réactualisant dans la « matrice » de William Gibson (GIBSON, 1984), la « schismatrice » de Bruce Sterling (STERLING, 1989) ou encore le « *Metaverse* » de Neal Stephenson (STEPHENSON, 1992). Ces imaginaires, parfois qualifiés de « cybercultures », constituent un sujet d'étude en soi, qui commence à être déblayé, les sociologues s'intéressant à leur maturation, à leur contenu et à leur réception (BELL & KENNEDY, 2000 ; BURROWS & FEATHERSTONE, 1995 ; CAVALLERO, 2000 ; FLICHY, 2001 ; JORDAN, 2001 ; RIGAUT, 2001).

Le cyberespace rassemble donc *conceptuellement* plusieurs espaces virtuels aux rythmes, à l'histoire, aux fonctions et aux représentations distincts, dont certains préexistaient à l'internet. Cet « espace » suit un modèle de développement cumulatif, plutôt que substitutif, l'apparition d'un nouveau média tel qu'internet conduisant à l'apparition d'espaces virtuels qui s'additionnent à ceux qui leur préexistaient plutôt qu'ils ne s'y substituent. Josiane Jouet insiste ainsi sur le fait que « l'usage social des TIC se construit

technologies deviennent plus conviviales. Malgré les évolutions des années 1990, elles demeurent coûteuses, encombrantes et encore peu convaincantes.

dans son interrelation avec les usages des autres machines à communiquer » (JOUET, 2000 : 501-502), ce que confirment Kevin Hill et John Hughes, pour qui « les gens utilisent l'internet de la même manière et pour les mêmes raisons que les médias plus traditionnels. (…) l'internet ne change pas les gens, il leur permet simplement de faire les mêmes choses différemment » (HILL & HUGHES, 1998 : 44).

Malgré l'amélioration technique des interfaces les reliant au monde réel, tous ces espaces virtuels continuent de s'en distinguer par leur incomplétude. Quoi qu'en disent les anciens acteurs de la contre-culture américaine des années 1960, recyclés dans le « cyber-utopisme », dont Timothy Leary fut le porte-parole, hypnotisé par la prétendue « hypersensualité » de l'ordinateur (LEARY, 1994), tout espace virtuel est partiel, imitant le réel mais échouant à le reproduire. La « simultanéité déspatialisée » (THOMPSON, 2000 : 198) permet sans doute de s'entendre et de se voir à distance, mais les « *teledildonics* » (c'est-à-dire le sexe virtuel)[7] n'ont jamais acquis la dimension tactile dont rêvaient sociologues et pornographes ; le « cybersexe » relève moins de l'expérience sensible que philosophique puisqu'il se place « en dehors de la sexualité, dans l'évitement du contact réel avec l'Autre, dans l'absence de sécrétion, dans une sensualité désincarnée et discursive » (FRAU-MEIGS, 1996 : 56). Le virtuel, note avec justesse Marc Guillaume, est un monde « sans odeur, sans saveur et sans chaleur », qui n'est en fait ni plus ni moins que le réel mais tout simplement autre (*ibid* : 62).

Ainsi de nouveaux modes de « spatialité », c'est-à-dire de construction sociale de l'espace, s'inventent-ils actuellement en ligne, étant entendu que les lieux sur lesquels ils s'appuient diffèrent notablement des espaces géographiques classiques, « dans la mesure où l'on peut y accéder de n'importe quel endroit (si tant est que l'on soit équipé de la technologie adéquate), où ils sont basés sur de nouveaux modes d'interaction, de nouvelles formes de relations sociales, et où ils se trouvent organisés autour d'affinités et d'intérêts communs plutôt que d'une coïncidence de localisation » (DODGE & KITCHIN, 2001 : 17). Pour certains observateurs des communautés virtuelles, le cyberespace réconcilierait en fait *gemeinschaft* et *gesellschaft* dans une série de lieux métaphoriques, informels, décentralisés et auto-gérés (RHEINGOLD, 1993). Les spatialités « proto-géométriques » stimulées par le cyberespace dessinent effectivement des « essences morphologiques vagues, c'est-à-dire vagabondes ou nomades » (DELEUZE & GUATTARI, 1981 : 454), qui peuvent prendre la forme des « zones autonomes temporaires » (TAZ) théorisées par Hakim Bey : « la TAZ est comme une insurrection sans engagement direct contre l'État, une opération de guérilla qui

[7] Ce néologisme est dû au sociologue Ted Nelson ; un « *dildo* » est un gode en anglais.

libère une zone (de terrain, de temps, d'imagination) puis se dissout, avant que l'État ne l'écrase, pour se reformer ailleurs dans le temps ou l'espace. » (BEY, 1985) Ces nouveaux espaces échappant partiellement, et surtout temporairement, au contrôle étatique, sur le modèle des « quasi-Etats » établis par les pirates du XVIIe-XVIIIe siècle (THOMSON, 1994 : 46), ne se sont pas pour autant coupés des lieux tangibles de la géographie euclidienne : « en réalité, de nombreux sites et projets [télématiques] cherchent à reconnecter et à revigorer des communautés spatiales en encourageant l'interaction entre les résidents d'un espace donné. » (DODGE & KITCHIN 2001 : 17) Ainsi, sociabilités présencielles et distancielles, loin de s'exclure, se complètent chaque jour un peu plus dans nos vies publiques et privées, renforçant les processus d'irruption du distant dans le local et, rétroactivement, amplifiant les résonances à distance des évènements locaux (GIDDENS, 1991 : 187).

Remarques méthodologiques et pistes de recherche

L'étude des usages, politiques ou non, de l'internet, pose un certain nombre de problèmes méthodologiques au chercheur en sciences sociales. Le premier est bien sûr celui de l'identification et de la vérification des sources, en ce qui concerne les données hypertextuelles, ainsi que les identités, en ce qui concerne les interlocuteurs. Il est possible de recouper les informations obtenues sur le net avec d'autres provenant de médias traditionnels, mais il est beaucoup plus difficile de vérifier l'authenticité d'un site et la localisation de ses commanditaires. En outre, comme le fait remarquer Peter Dahlgren, « l'anonymat sur l'internet facilite la tromperie » (DAHLGREN, 2000 : 178), ce qui rend les données recueillies lors de *chats* en ligne, par *e-mails* ou sur des forums de discussion particulièrement délicates à utiliser. Fabien Granjon, estimant qu'après tout il n'existe pas plus de raison pour que les individus mentent en ligne que dans le monde réel, a choisi le principe d'un questionnaire diffusé et récupéré électroniquement auprès de 250 internautes dans son enquête sur l'usage de l'internet par les nouveaux mouvements sociaux français. Il a complété ces données par une série d'entretiens semi-directifs, menés hors ligne, et par l'étude de 15 listes de diffusion animées par des organisations représentatives de la « critique sociale par projets » (GRANJON, 2001). Cet équilibre entre données quantitatives et qualitatives, que l'on constate dans la plupart des études sur les usages d'internet (DAVIS, 1999 ; POISSENOT & SADOUDI, 2000), est également préconisé par Josiane Jouet, qui suggère que « seule l'approche qualitative peut tenter de dégager la signification

des actes de communication au niveau individuel et le sens social des usages auprès de groupes sociaux spécifiques », avant d'ajouter que « le cadrage statistique permet [quant à lui] de faire ressurgir les phénomènes de segmentation sociale, le poids des variables démographiques […] et de découvrir, par l'analyse de données, les facteurs du changement social et les modes d'inscription de l'usage dans les rapports sociaux globaux » (JOUET, 2000 : 514). Quoi qu'en disent ces auteurs, le recueil de données quantitatives en ligne est cependant problématique. Outre le problème de l'anonymat, évoqué plus haut, il faut aussi mentionner la nature biaisée des résultats recueillis à partir d'enquêtes en ligne : les individus prêts à répondre sont généralement des internautes assidus ou « des *innovateurs* qui ne représentent pas plus qu'un petit cinquième de la population et ont tendance à donner des réponses positives, ce qui gonfle vers le haut les enquêtes » (LAFRANCE, 1996 : 174).

Olivier Roy, dans son étude de « l'oummah virtuelle », s'est pour sa part livré à une étude du contenu d'un certain nombre de sites islamiques émanant d'un individu ou d'un groupe d'individus, portant une attention particulière aux liens entre ces pages artisanales et d'autres sites. L'« obésité informationnelle » qui est le pendant de la richesse du web (GUILLAUME, 2000 : 67) rend cependant impossible une enquête quantitative sur un phénomène tel que l'islam en ligne, « à moins de mobiliser plusieurs chercheurs dans un espace de temps resserré (et à plein temps) ». La durée de vie limitée d'un grand nombre de sites, en particulier des pages personnelles, rend par ailleurs vaine toute entreprise de ce type, puisque « les données recueillies une année ne feront pas toujours sens quelques mois après » (ROY, 2000 : 231). L'internet, tel le livre de sable de Borges, n'est jamais semblable à chaque consultation. A moins de télécharger chaque page consultée au fil de la navigation, il est impossible de s'assurer que l'on pourra retrouver trace d'un site visité, ce qui rend naturellement difficile de « prouver que vous avez bien vu ce que vous prétendez avoir vu sur l'internet », ainsi que le note Richard Davis dans les remarques méthodologiques qui viennent clore son étude de l'impact de l'internet sur la vie politique américaine (DAVIS, 1999 : 187).

Outre ces problèmes méthodologiques généraux que pose l'internet au sociologue ou au politologue, celui-ci se trouve confronté à une difficulté supplémentaire lorsqu'il souhaite s'intéresser aux pratiques de contestation qui prennent appui sur les technologies du cyberespace : celle de la prise de contact avec des individus engagés dans des activités illégales, qui rechignent naturellement à se confier à un inconnu. Peter Taylor est à ce jour le seul sociologue qui soit parvenu à conduire une véritable enquête de terrain sur la « scène » *hacker*. Purement qualitative, celle-ci repose sur une méthode originale. Les premiers contacts de l'auteur au sein de la « scène » et de l'industrie de la sécurité informatique ont

été obtenus sur le net, par le biais de courriers électroniques. Par un effet « boule de neige », ces premiers contacts ont permis à Taylor de rencontrer d'autres individus *de visu*, ce qui lui a ensuite permis de prendre d'autres contact par e-mails, et ainsi de suite, dans une ronde permanente entre le monde « réel » et l'internet. En Grande-Bretagne, l'entrée en vigueur du Computer Misuse Act a rendu impossible toute enquête de terrain digne de ce nom et Taylor a donc choisi de focaliser ses recherches sur les Pays-Bas, les *hackers* néerlandais étant plus disposés à évoquer leurs activités illégales que leurs camarades britanniques. Il a cependant été impossible à l'auteur d'interviewer des concepteurs de virus ou de vers informatiques, dans la mesure où « même ceux qui acceptent d'évoquer leurs intrusions informatiques illicites se refuseront toujours à admettre leur implication dans la diffusion de virus » (TAYLOR, 1999 : x).

Ces écueils ne doivent pas détourner les chercheurs en sciences sociales de l'internet et de ses usages politiques, contestataires comme disciplinaires. De nombreuses pistes de recherche s'offrent aujourd'hui à eux. La première, qui séduira les internationalistes, est celle de la régulation mondiale de l'internet, qui pourrait notamment être saisie à travers les activités de l'ICANN (Internet Corporation for Assigned Names and Numbers), l'organisation responsable de la gestion des noms de domaine sur le *web*. Une deuxième piste de recherche, qui pourrait mobiliser certains sociologues, consisterait en une étude comparative d'une série de *webmasters* issus de diverses organisations, qui viserait à déceler le degré d'implication politique et le rôle exact de ces techniciens au sein de celles-ci. Le travail de Flore Trautmann sur le webmestre d'Attac, Laurent Jesover, a posé les jalons d'une sociologie de ces architectes du net, mais celle-ci demande à être poursuivie et enrichie par une réflexion comparative. Une autre piste de recherche est l'étude des « cyber-cultures » qui se sont développées sur le net : quelles représentations de la *polis* véhiculent-elles et comment ces imaginaires de l'internet s'actualisent-ils dans des pratiques courantes et des usages innovants ? Les travaux de Patrice Flichy ont déjà permis de repérer le pouvoir performatif des imaginaires d'internet (FLICHY, 2001), mais la question mériterait de plus amples recherches, à nouveau dans une perspective comparative. Il serait, en dernier lieu, intéressant de se lancer dans une expérience d'observation participante à l'occasion d'une manifestation de protestation en ligne, qui conduirait à se familiariser en temps réel avec un logiciel « hacktiviste » puis à décrire minutieusement le déroulement de l'opération et le type (ou l'absence) d'interactions s'instituant entre les participants. Ce sont de telles « *thick descriptions* » qui font encore défaut aux études sur les « politiques de l'internet ».

La contestation dans le cyberespace prend diverses formes, et toutes ne sauraient être qualifiées de « hacktivisme ». Le terme, inventé par les *hackers* du Cult of the Dead Cow (cDc), désigne « la convergence du *hacking* et de l'activisme, le *hacking* désignant ici les opérations mettant à profit les ordinateurs de manière inhabituelle et souvent illégale, notamment à l'aide de logiciels spéciaux [*hacking tools*] » (DENNING, 2001 : 263). Pour ses acteurs, le hacktivisme relève de la « désobéissance civile électronique » et il ne saurait être placé sur le même plan que le « cyberterrorisme », si tant est que celui-ci représente une menace effective. Les réflexions apparues depuis quelques années sur « l'infoguerre » demandent en effet à être traitées avec prudence. Le concept de « *netwars* »[8] qui se banalise actuellement est dû aux analystes de la RAND[9] et du Center for Strategic and International Studies (CSIS)[10] qui, au début des années 1990, voyaient les cyberconflits pointer à l'horizon et cherchaient à alerter les autorités militaires américaines sur cette nouvelle menace. En 1994, le CSIS publia ainsi un rapport où l'on pouvait lire : « un despote armé d'un ordinateur et d'une petite équipe de *hackers* expérimentés peut s'avérer aussi dangereux que n'importe lequel des adversaires auxquels nous nous sommes trouvés confrontés depuis la seconde guerre mondiale » (cité par TAYLOR, 1999 : 7). Dix ans plus tard, force est de constater que la menace cyberterroriste ne s'est pas matérialisée, alors que le hacktivisme s'est banalisé, mêlant engagement politique, esprit ludique et performance artistique.

[8] Il s'agit d'attaques sur des systèmes d'information déclenchées par deux grands types d'acteurs : « terroristes et criminels » et « activistes sociaux » ; cf. ARQUILA, & RONFELDT, 2001.

[9] Créé par l'US Air Force en 1946, ce *think tank* basé à Santa Monica est spécialisé dans l'analyse des enjeux stratégiques des technologies de l'information ; l'acronyme RAND a été obtenu par contraction de « *research and development* » ; sur l'histoire de la RAND, cf. http://rand.org/about/.

[10] Initialement associé à l'Université de Georgetown, à Washington, ce centre de recherche s'en est autonomisé et il est devenu l'un des *think tanks* les plus influents des Etats-Unis en matière de politique étrangère. Sur l'histoire du CSIS, cf. http://csis.org/about/index.htm.

Les noces du militantisme et de l'« *underground* informatique »[11]

Le hacktivisme procède d'abord d'une rencontre entre deux groupes sociaux jusqu'alors étrangers l'un à l'autre : « l'*underground* informatique » et les héritiers de la contre-culture des années 1960-1970. Le concept de « désobéissance civile électronique » fut ainsi théorisé par cinq artistes et intellectuels américains rassemblés dans le Critical Art Ensemble (CAE). Fondé en 1987, ce groupe d' « usagers tactiques des médias »[12] s'est rendu célèbre par ses performances artistiques, notamment par ses expériences de théâtre interactif (ou « recombinatoires »[13]) destinées à alerter l'opinion publique américaine sur les dangers des biotechnologies, ainsi que par ses essais théoriques. Le plus fameux d'entre eux reste *The Electronic Disturbance*, publié en 1993, qui s'ouvre sur ces mots :

> Les règles de la résistance culturelle et politique ont radicalement changé. La révolution technologique induite par le développement rapide de l'ordinateur et de la vidéo a façonné une nouvelle géographie des relations de pouvoir dans le premier monde, qui aurait été tout simplement impensable il y a seulement vingt ans : les gens se trouvent réduits au rang de donnée, la surveillance opère désormais à une échelle globale, les esprits sont asservis à la réalité défilant sur les écrans, et un pouvoir autoritaire émerge qui prospère sur l'absence. La nouvelle géographie est une géographie virtuelle, et le noyau dur de la résistance culturelle et politique doit s'affirmer dans l'espace électronique. (Critical Art Ensemble, 1994 : 3)

Si l'on a pris l'habitude de voir dans ce texte la première théorisation de la « désobéissance civile électronique », force est de constater que ses auteurs s'inspirent plus des principes de l'action révolutionnaire que des préceptes de Thoreau :

> Un groupe réduit mais bien coordonné de *hackers* pourrait introduire des virus électroniques et des bombes logiques dans les banques de données, dans les programmes et les réseaux de l'autorité (…). Une telle action ne requiert pas d'action de classe unitaire, non plus qu'une action simultanée dans plusieurs localités. Les éléments moins nihilistes pourraient ressusciter les stratégies d'occupation en retenant l'information, et non plus la propriété, en otage. (*ibid* : 25)

Les membres du CAE sont néanmoins conscients des difficultés que pose l'extension de l'action révolutionnaire au cyberespace. Au premier rang de celles-ci figurerait la nature « dépolitisée » des *hackers*, essentiellement motivés par le « vandalisme ludique », « l'espionnage », ou « le désir de revanche personnelle contre une source d'autorité donnée » (*ibid*). Les membres du Critical Art Ensemble constatent, non sans amertume, que l'éthique *hacker* est fondamentalement hostile à la déstabilisation du cyberespace, auquel les *hackers* ont contribué à donner naissance et grâce auquel ils prospèrent aujourd'hui. Le recours au « cybotage » reviendrait, pour ces individus, à scier la

[11] Ce terme, apparu dans des magazines emblématiques de la cyberculture tels que *Mondo 2000*, a été repris par JORDAN & TAYLOR, 1998.

[12] Ainsi qu'ils se définissent eux-mêmes dans une interview en ligne : cf. http://www.lumpen.com/magazine/81/critical_art_ensemble.shtml.

[13] Cf. http://www.virtualistes.org/cae1.htm#theatre.

branche sur laquelle ils s'appuient. Les membres du CAE réfléchissent alors aux moyens susceptibles de rallier non pas l'ensemble de la classe des « cybertravailleurs », mais d'en coopter une poignée, tout en confiant aux « artistes-activistes » le soin de théoriser « un discours critique sur ce qui est précisément en jeu dans le développement de cette nouvelle frontière » et de « construire un forum public pour une spéculation opérant sur le mode de la résistance » (*ibid* : 27). Deux ans plus tard, le groupe compléta cette réflexion par la première théorisation explicite de la « désobéissance civile électronique », dans un texte intitulé « Electronic Civil Disobedience and other Unpopular Ideas ». Les auteurs, se revendiquant de Thoreau, Bey, Deleuze et Guattari, y définissent la « désobéissance civile électronique » comme « de nouvelles formes de perturbation qui s'en prennent aux (non-) centres du pouvoir au niveau électronique »[14]. Les membres du CAE préfèrent aujourd'hui à ce concept celui de « résistance numérique » (*digital resistance*), qui se réfère dans leurs textes aux « usages tactiques des médias », c'est-à-dire à « un usage et une théorisation critiques des médias qui reposent sur l'ensemble des médias, des plus vieux aux plus jeunes, de manière lucide et originale, afin de remplir un certain nombre d'objectifs non-commerciaux et de médiatiser toutes sortes de questions politiques subversives »[15].

Les réflexions du Critical Art Ensemble auraient pu demeurer de sympathiques élucubrations situationnistes sans grande incidence politique si l'aggravation du conflit du Chiapas ne leur avait offert une caisse de résonance. Suite au massacre d'Acteal de 1997, nombre d'activistes du monde « réel » décidèrent de compléter leurs mobilisations traditionnelles par des actions en ligne. Si certains de ces acteurs usaient déjà de l'internet à des fins d'information ou de médiatisation (WARKENTIN, 2001), c'est à une organisation pro-zapatiste que l'on doit l'organisation de la première grande campagne de protestation de grande ampleur *sur* et non plus seulement *au moyen de* l'internet[16]. En 1998, l'Electronic Disturbance Theater (EDT) mit au point la technique du « *sit-in* virtuel », consistant à freiner ou à bloquer l'accès à un site internet par le biais d'un programme spécifique, baptisé FloodNet. Son principe est le suivant : en consultant l'un des sites internet de l'EDT, le navigateur de l'internaute télécharge automatiquement le logiciel qui, une fois activé, connecte de façon répétée l'internaute à un ou plusieurs sites cibles. Le 9 septembre 1998, 10 000 personnes dispersées à travers le monde participèrent ainsi à un *sit-in* virtuel contre les sites internet du Président mexicain Ernesto Zedillo, du Pentagone, de la bourse de

[14] http://www.virtualistes.org/cae2.htm#desobeissance.

[15] http://amsterdam.nettime.org/Lists-Archives/nettime-l-0203/msg00158.html.

[16] Encore que le groupe Strano Network soit à l'origine de la première « *net strike* », qui consista en une attaque sur un certain nombre de sites gouvernementaux français le 21 décembre 1995, en signe de protestation contre les essais nucléaires du pays dans le Pacifique.

Francfort et de la School of Americas, inondant chacun d'entre eux de 600 000 connections par minute (DENNING, 2001 : 265). D'un point de vue strictement technique, cette campagne révéla les faiblesses de l'EDT face à des agences gouvernementales qui se préparent depuis longtemps à l'« infoterrorisme ». Les programmeurs du Pentagone répliquèrent en « gelant » FloodNet en l'espace de quelques heures[17] et les responsables du site de Zedillo mirent au point une contre-attaque lors d'un autre *sit-in* virtuel organisé en juin 1999. Le site de la bourse de Francfort, quant à lui, ne se trouva guère affecté par ces connections supplémentaires, dans la mesure où il reçoit habituellement 6 millions de connections quotidiennes. L'opération ne fut pas pour autant un échec. Les militants de l'EDT, à l'instar de ceux du CAE, envisagent la « protestation électronique » comme une performance à la fois politique et artistique. Le programme FloodNet permet de ralentir l'accès à un site internet mais aussi de substituer au message d'erreur du serveur celui de son choix : en tapant « *human rights* » sur la page des « messages personnels » accompagnant FloodNet, l'usager transformait par exemple le message d'erreur en « *human_rights not found on this server* ». Le concepteur de FloodNet, Brett Stalbaum, l'a en fait conçu comme « une forme d'art conceptuel sur le net qui met le pouvoir entre les mains des gens par l'intermédiaire de l'expression active/artistique », mais également comme « une manière de nous souvenir et d'honorer la mémoire de ceux qui ont donné leur vie pour défendre la liberté »[18]. Le « succès » des opérations hacktivistes de l'EDT ne saurait donc être mesuré en termes purement techniques (peuvent-elles bloquer des sites, menacer les infrastructures communicationnelles nationales ou globales, etc. ?) puisqu'elles incluent une dimension esthétique évidente, engagement politique et performance artistique se confondant dans la protestation en ligne. De telles opérations sont également conçues comme des « moments de subjectivation » destinés à construire un sentiment d'appartenance commune pour des usagers actifs dispersés à travers le monde. Ainsi FloodNet a-t-il été explicitement conçu comme une réponse au « syndrome du *hacker* solitaire », aveuglé et isolé par son « génie malade »[19]. En attirant l'attention des médias (notamment par le biais d'une « une » du *New York Times* consacrée à ses activités), l'EDT estima par ailleurs avoir rempli son principal objectif politique, à savoir « aider le peuple du Chiapas à conserver la reconnaissance internationale dont il a besoin pour survivre » (cité par DENNING, 2001 : 266). Ces propos des responsables de l'EDT révèlent deux caractéristiques essentielles de la « protestation numérique » : (1) celle-ci vise

[17] « Pentagon deflects web assault », *Wired News*, 10 septembre 1998, disponible à l'adresse suivante : http://www.wired.com/news/politics/0,1283,14931,00.html.

[18] http://www.thing.net/~rdom/ecd/ZapTact.html.

[19] *ibid*.

essentiellement à capter l'attention des médias traditionnels ; (2) elle ne saurait opérer sans relais *offline*, eux-mêmes renforcés par leurs ramifications dans le cyberespace. Cette dépendance mutuelle des tactiques de protestation dans l'espace « local-réel » et « global-virtuel » ne traduit pas une dialectique entre deux spatialités essentialisées. Au contraire, en interagissant, ces deux pôles de la subjectivation et de la protestation se transforment mutuellement au point qu'il devient difficile de les isoler. Ainsi, c'est le « zapatisme digital » qui a porté la cause chiapanèque à la connaissance des fondateurs de l'EDT et qui, selon eux (on pourrait contester ce point mais tel n'est pas ici notre sujet), a permis à l'Armée zapatiste de libération nationale (EZLN) du sous-commandant Marcos de se prémunir de l'annihilation face à « un adversaire supérieur en nombre et équipé des dernières technologies en matière de lutte anti-drogue » (*ibid*). Ce sont donc les relais cyberspaciaux du conflit initialement localisé du Chiapas qui ont contribué à la mobilisation des fondateurs de l'EDT, eux-mêmes préalablement politisés *offline*. Le cyberespace, tout aussi virtuel qu'il soit, apparaît ici comme une vaste interface entre luttes locales, véritable équaliseur de griefs spécifiques et de conflits jusqu'alors étrangers les uns aux autres. En contribuant à l'interconnexion de micro-politiques initialement localisées, à travers de véritables « internationales électroniques » ou par le biais de « coalitions » plus souples et à la durée de vie plus limitée (BADIE, 2002 : 290), les nouveaux réseaux télématiques participeraient alors à l'émergence d'un véritable « espace public international », que Bertrand Badie définit comme « l'ensemble des interactions extraétatiques qui s'opèrent sur la scène internationale afin d'en produire les enjeux, d'en assurer la publicité, d'orienter les opinions qui s'y expriment et donc de participer à l'élaboration des politiques qui la structurent » (*ibid*, 273). Même si l'extension à l'international de notions comme « espace public » peut paraître périlleuse, tout autant que celle de « société civile » (POULIGNY, 2001), il convient de relever la faculté « coagulante » de l'internet, qui permet à des militants de tous bords et de tous lieux d'unir leur force en vue d'une action ciblée, en ligne ou hors ligne, ou d'établir une collaboration sur une plus longue durée. Cette faculté « coagulante » de l'internet est décisive car elle atténue l'incommunicabilité des luttes contemporaines, qui « ont gagné en intensité ce qu'elles ont perdu en extension, en durée et en communicabilité » (NEGRI & HARDT, 2000 : 85).

Pour les militants de l'EDT, comme pour certains « cyberlibertariens » tels que John Perry Barlow[20], l'internet constitue également un outil particulièrement efficace pour braver la

[20] Cet ex-parolier du Grateful Dead et fondateur de l'Electronic Frontier Foundation croit en « la promesse d'un nouvel espace social, global et anti-souverain, où chacun, partout, peut sans crainte faire part de ce qu'il pense au reste de l'humanité » (cité par LOADER, 1997 : 4).

souveraineté des Etats. Ainsi les membres de l'EDT affirment-ils dans leur « Call for FloodNet Action for Peace in the Middle East » :

> Nous ne croyons pas que seuls les Etats-nations aient l'autorité légitime permettant de s'engager dans une guerre ou une agression. Et nous considérons le cyberespace comme un moyen pour les acteurs politiques non-étatiques de s'ingérer dans les zones présentes et à venir de conflits et ce, en transcendant les frontières [cité par DENNING, 2001 : 267].

S'il est encore trop tôt pour proclamer la disparition de l'Etat, comme n'hésitent pas à le faire les cyberlibertariens (FLICHY, 2001 : 205-212), il est indéniable que l'internet participe à l'essor et au rapprochement de divers « réseaux revendicatifs » translocaux (*advocacy networks*), que Margareth Keck et Katryn Sikkink définissent comme « les acteurs opérant internationalement sur une question donnée, qui se trouvent liés par des valeurs partagées, par un discours commun et par un échange dense d'informations et de services » (KECK & SIKKINK, 1998 : 2). Il s'agit notamment des « communautés épistémiques », des mouvements sociaux locaux, des fondations privées, des médias, des églises, de certaines fractions d'organisations régionales et internationales ainsi que de l'exécutif ou du pouvoir parlementaire de certains Etats. Ces réseaux revendicatifs, dont les origines remontent au mouvement abolitionniste et à celui des suffragettes (KECK & SIKKINK, 2000), s'organisent autour de trois fonctions : (1) des politiques communicationnelles (*information politics*), consistant en « la capacité à générer rapidement une information crédible et politiquement utile et à la diffuser là où elle est susceptible d'avoir le plus grand impact » ; (2) des politiques symboliques, consistant en « la capacité à jouer sur des symboles, des actions ou des histoires qui éclairent une situation pour une audience généralement éloignée » ; (3) des politiques du levier (*leverage politics*), témoignant de « la capacité à interpeller des acteurs puissants pour affecter une situation où des maillons plus faibles d'un réseau risquent d'avoir peu d'influence » (KECK & SIKKINK, : 2 ; 9). L'usage de l'internet par ces « réseaux revendicatifs », et notamment par les ONG, a fait l'objet de plusieurs études ces dernières années, dont la dimension critique mérite d'être mentionnée (CAPLING & NOSSAL, 2001 ; POULIGNY, 2001 : 166-167). Les travaux les plus sérieux insistent notamment sur la persistance d'une « fracture numérique », c'est-à-dire d'un accès inégal des populations et des acteurs sociaux à l'internet, tant au niveau national qu'international, qui limite considérablement son caractère démocratique et sa contribution à l'avènement d'une hypothétique « société civile globale » (WARKENTIN, 2001 : 33-35).

Le hacktivisme, stratégie du désordre

Si la légalité des « *sit-in* virtuels » peut être questionnée[21], d'autres formes de hacktivisme transgressent de façon plus évidente les lois en vigueur dans le cyberespace, ces dernières les assimilant en retour à des formes de « cybercrime » ou de « cyberterrorisme ». Tel est notamment le cas des attaques par « déni d'accès » (DOS)[22] ou par « *e-mail bombing* ». Cette seconde technique permet de bloquer un site en le « bombardant » littéralement de courriers électroniques, au moyen de logiciels spécifiques. En juin 1998, un groupe probablement lié à la guérilla des Tigres tamouls (LTTE) attaqua ainsi les sites internet de plusieurs ambassades sri-lankaises. L'attaque consista en 800 e-mails envoyés quotidiennement à chaque site, où l'on pouvait lire : « Nous sommes les Internet Black Tigers et nous faisons cela pour couper vos communications » (cité par DENNING, 2001 : 269). Durant le conflit du Kosovo, cette arme fut également employée à l'encontre du site de l'OTAN, mais les résultats avérés de ces attaques, autant que leur provenance, demeure sujet à caution. En représailles à celles-ci, un résident de Californie, Richard Clarke, entreprit quant à lui de fermer le site du gouvernement yougoslave. Il y parvint en quelques jours, au moyen de 500 000 e-mails. Ce coup d'éclat ne fut pourtant pas du goût de son fournisseur d'accès, Pacific Bell, qui annula le contrat du jeune homme. Le fournisseur d'accès Institute for Global Communications (IGC) fut également victime d'une attaque par « *e-mail bombing* » en 1997 parce qu'il hébergeait le site de l'*Euskal Herria Journal*, favorable à l'indépendance du Pays basque. L'IGC ferma le site le 18 juillet, non sans avoir pris soin de l'archiver pour lui permettre de réapparaître sous forme de sites « miroirs ». Le porte-parole de l'Internet Freedom Campaign, qui contribua à cette opération, déclara à cette occasion : « le Net doit permettre de lire toutes sortes d'informations controversées et d'en débattre » (cité par *ibid*). Malgré cette initiative, un mois après la fermeture du site par l'IGC, Scotland Yard fit fermer celui de la branche britannique de l'ONG Internet Freedom pour avoir, à son tour, hébergé le journal basque. A quoi l'ONG répondit simplement qu'elle transférerait les pages sensibles sur le site de sa branche américaine.

Les pratiques de « *defacement* », qui consistent à « défigurer » la page d'accueil d'un site, sont également prisées par les hacktivistes. En septembre 1998, un groupe de *hackers* portugais « défigura » ainsi 40 sites indonésiens en y « tagant » « *Free East Timor* » et en y

[21] Aux Etats-Unis, les lois fédérales interdisent de distribuer un programme ou un code source dans l'intention de causer des dommages à un site. Le discours de l'EDT et des Electrohippies [cf. infra] est pourtant résolument légaliste, se distinguant par là de celui du Critical Art Ensemble.

[22] Les attaques par DOS consistent à bloquer l'accès à un site en déroutant les connections à celui-ci.

ajoutant des liens vers des sites documentant les violations des droits de l'homme attribuées aux autorités indonésiennes au Timor oriental. En juin 1998, en guise de protestation aux essais nucléaires indiens, un groupe international de *hackers* baptisé Milw0rm attaqua quant à lui le site web du Bhaba Atomic Research Center (BARC) et remplaça sa page d'accueil par une photographie d'un champignon atomique accompagné de la légende « si une guerre nucléaire éclate, vous serez les premiers à hurler… ». Les jeunes gens, qui affirmèrent agir par conviction politique autant que « pour le frisson », revendiquèrent également le vol de plusieurs milliers de pages de courriers électroniques et de documents de recherche, notamment des échanges épistolaires entre les responsables du programme nucléaire indien et certains officiels israéliens. Les six *crackers* étaient âgés de 15 à 18 ans et étaient originaires des Etats-Unis, de Grande-Bretagne, des Pays-Bas et de Nouvelle-Zélande[23]. En juillet 1998, les mêmes pirates unirent leurs forces à celles du groupe Ashtray Lumberjack dans le cadre d'une attaque qui toucha plus de 300 sites, les internautes souhaitant s'y connecter se trouvant redirigés vers le site de Milw0rm où ils se trouvaient accueillis par un message anti-nucléaire. De nombreux sites furent également victimes d'actions de piratage durant le conflit du Kosovo. Le groupe de *hackers* américains Team Spl0it s'attaqua par exemple à plusieurs sites des autorités yougoslaves en y postant des messages tels que « Dites à votre gouvernement de mettre un terme à la guerre ». Le Kosovo Hackers Group, coalition de *hackers* européens et albanais, défigura quant à lui au moins cinq sites avec des bannières rouges et noires proclamant « *Free Kosovo* ». L'agence de presse serbe SRNA rapporta que, de leur côté, les membres du groupe Black Hand réussirent à effacer des données d'un ordinateur de l'U.S. Navy. Les membres de ce groupe revendiquèrent également la mise hors service d'un site favorable à l'indépendance du Kosovo en affirmant : « Nous n'aurons de cesse de nettoyer l'internet des mensonges albanais ». L'attaque de la Black Hand contre le journal nationaliste croate Vjesnik déclencha quant à lui une contre-attaque des hacktivistes croates sur la Bibliothèque nationale serbe en octobre 1998[24]. Le bombardement de l'ambassade de Chine à Belgrade par les forces de l'OTAN suscita de son côté la colère des *hackers* chinois, qui répliquèrent en défigurant les sites de l'ambassade américaine à Pékin, ainsi que des Départements américains de l'Intérieur et de l'Energie. De leur côté, certains *hackers* américains s'en sont pris à des serveurs gouvernementaux chinois ou ont apporté leur soutien à des groupes de « cyberdissidents » chinois tels que les Hong Kong Blondes, alliés au Cult of the Dead Cow et basés à Toronto, Montréal et Paris[25].

[23] « Crackers: We stole nuclear data », *Wired News*, 3 juin 1998.

[24] « 'Hacktivists' of all persuasions take their struggle to the Web », *The New York Times*, 31 octobre 1998.

[25] « Hacking in the name of democracy in China », *Toronto Star*, 4 juillet 1999.

En décembre 1998, les Américains de la Legion of Underground (LoU) allèrent jusqu'à déclarer une « cyberguerre » à la Chine et à l'Irak, appelant à la destruction totale du réseau informatique de ces deux pays. Cette annonce provoqua une vive réaction de la « scène » *hacker*. Début 1999, le magazine *2600*. *The Hacker Quarterly*, le Chaos Computer Club[26], le Cult of the Dead Cow (cDc), !Hispahack, L0pht Heavy Industries, Phrack, Pulhas, et plusieurs groupes néerlandais dénoncèrent le projet de la LoU. Reid Fleming, du cDc, déclara à cette occasion : « On ne peut légitimement espérer améliorer le libre accès à l'information en travaillant à la destruction des réseaux de données » (cité par DENNING, 2001 : 275). Devant ces protestations de leurs confrères, les membres de la LoU renoncèrent à leur projet, sans que l'on sache s'ils avaient effectivement les moyens de le mettre en oeuvre ou s'il ne s'agissait que d'un bluff destiné à s'attirer la reconnaissance des médias et de la « scène » *hacker*.

Certains hacktivistes ont également recours à des virus et des vers informatiques pour diffuser leurs messages protestataires. Dès 1989, un groupes d'opposants au nucléaire diffusa le vers « *Wank* » sur le réseau SPAN de la NASA, occasionnant des dégâts évalués à un demi-million de dollars. En février 1999, un adolescent israélien parvint quant à lui à faire fermer un site gouvernemental irakien en lui envoyant un *e-mail* accompagné d'un fichier attaché « empoisonné ».

On peut s'interroger sur l'efficacité de telles opérations. Ainsi de nombreux sites sensibles sont-ils désormais équipés de protection (les « *firewalls* », parfois développés par d'anciens *hackers*[27]) et les outils de « cyberdéfense »[28], mis au point ces dernières années par de nombreux gouvernements, réduisent la capacité de nuisance des opérations de

---

[26] Célèbre groupe de *hackers* allemands, basé à Hambourg et Berlin, opposé au hacktivisme et prêchant, à l'instar du cDc, la liberté de circulation totale de l'information sur le réseau.

[27] Le « roi du *phreaking* » lui-même, John Draper (alias « Cap'n Crunch »), s'est reconverti dans le développement de *firewalls* ; on pourra consulter son site, qui en dit long sur l'ambivalence de la relation qui lie les *hackers* à l'industrie de la sécurité informatique, cf. http://www.webcrunchers.com/crunch/.

[28] Les outils de cyberdéfense se sont développés ces dernières années avec l'encouragement des Nations Unies qui, en vertu de la résolution 53/70 de décembre 1998 de l'Assemblée générale sur les « développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale », invite ses membres à s'engager activement et à collaborer dans la lutte contre la « cybercriminalité ». En juillet 1996, le président Clinton a, quant à lui, annoncé la formation de la Commission sur la protection des infrastructures critiques, qui a rendu un rapport alarmiste en octobre 1997 sur les « cybermenaces » pesant sur les systèmes d'information américains. Le Department of Defense (DoD) est, depuis cette date, activement engagé dans des programmes de sécurisation des systèmes informatiques assurant le fonctionnement des « infrastructures critiques ». En 1998, le FBI s'est, de son côté, doté d'une section spécialement chargée de lutter contre la cybercriminalité et le cyberterrorisme : le National Crime Information Center (NCIC) ; à ce sujet, cf. CORDESMAN & CORDESMAN, 2002.

hacking politique. Celles-ci peuvent sans doute contribuer à médiatiser une cause oubliée et à instituer ou raviver des processus de collaboration entre mouvements sociaux à travers le monde (LEE, 1997), mais à la condition expresse de s'accompagner de contacts et de mobilisations hors ligne, comme le reconnaissent des groupes tels que l'EDT ou les Electrohippies [cf. infra]. Le succès politique des opérations hacktivistes dépend également des relais qu'elles trouvent au sein des médias traditionnels, dans la mesure où ceux-ci demeurent la principale voie d'accès à l'information de la plus grande partie de l'humanité. Au final, pour Dorothy Denning, « les hacktivistes peuvent s'enivrer de leur sentiment de puissance, parce qu'ils contrôlent les ordinateurs des gouvernements et suscitent l'attention des médias, mais cela ne signifie pas pour autant qu'ils parviennent à affecter les politiques publiques. Jusqu'à présent, un certain nombre d'exemples anecdotiques suggèrent au contraire que, dans la majorité des cas, ils y échouent ». Les formes légalistes d'activisme en ligne apparaissent en fait plus efficaces, dans la mesure où « de nombreuses études montrent que lorsque l'internet est utilisé de manière normale, et non déstabilisatrice, il peut constituer un outil efficace de l'activisme, surtout si son usage se trouve combiné à celui d'autres médias, tels que la télévision et la presse écrite, ainsi qu'à des rencontres avec les décideurs [dans le monde « réel »] » (DENNING, 2001 : 287-288).

Si son efficacité auprès des décideurs prête donc à question, le hacktivisme demeure en outre un mode de contestation peu consensuel auprès de ses acteurs potentiels. On assiste bien, depuis quelques années, à un rapprochement entre *hackers*, *crackers* et militants opposés à la mondialisation néo-libérale. A l'occasion de la rencontre de l'OMC de décembre 1999, les sympathisants des Electrohippies ont ainsi cherché à fermer le site de l'organisation au moment où se déroulaient des manifestations plus traditionnelles à Seattle (celles-ci furent cependant préparées sur l'internet par la People's Global Action). En janvier 2001, des hacktivistes anonymes ont quant à eux dérobé puis diffusé sur CD-ROM les numéros de cartes de crédit et de téléphone de 1400 VIPs réunis au forum de Davos, notamment ceux de Bill Clinton, de Li Peng, de Yasser Arafat, etc. La majorité des grandes ONG internationales demeurent cependant réticentes à user de méthodes illégales pour médiatiser leur cause. La webmestre d'Amnesty International, Susan Forste, a ainsi déclaré en novembre 2000 : « Je suis sûre qu'Amnesty n'aura pas recours à l'hacktivisme. Surtout si cela implique des activités illégales »[29]. Au sein de la « scène » elle-même, l'usage politique du *hacking* et surtout du *cracking* (piratage proprement dit) se trouve à la source d'une vive polémique. Celle-ci suggère clairement l'irréductibilité du *hacking* au politique, limitant

[29] « Hacking with a conscience is a new trend », *San Francisco Chronicle*, 20 novembre 2001.

considérablement son potentiel réformateur et invalidant par là même la prophétie des « cyber-zapatistes » selon lesquels « la Révolution sera numérisée ! »[30]

P@rtisans ou techno-traîtres ? L'irréductibilité du *hacking* au politique

Comme le soupçonnaient les membres du Critical Art Ensemble, le principal obstacle aux stratégies de protestation électronique tient au rapport ambigu, voire hostile, que les *hackers* entretiennent au politique. Ainsi la question du « hacktivisme » se trouve-t-elle actuellement au cœur d'une violente controverse au sein de la « scène ». Le néologisme est en effet dû à un membre du Cult of the Dead Cow, « Omega », qui le conçut pour railler les actions de protestation en ligne. Pour les membres du cDc, le terme aurait ensuite été récupéré « par de nombreux journalistes, par les ténors en déclin de la gauche et finalement par les *script kiddies* »[31]. Initialement ironique, le terme s'est donc banalisé suite à un renversement sémantique, auquel ont largement contribué les Electrohippies. Avec ceux de l'Electronic Disturbance Theatre, les membres de ce collectif d'activistes britanniques ont en effet participé à la théorisation et à la mise en pratique des techniques de « désobéissance civile électronique ». Les Electrohippies opèrent essentiellement par « déni d'accès distribué » (DDOS), qui vise à bloquer un site en déroutant les internautes s'y connectant, en respectant trois principes d'action : (1) proportionnalité (adéquation du dommage causé à la nocivité de la cible et mobilisation sur un point déterminé plutôt que contre l'organisation dans son ensemble) ; (2) palliation au déficit d'information (en informant les attaquants comme les victimes) ; (3) transparence (chaque attaquant devant révéler sa véritable identité)[32]. En décembre 1999, le collectif britannique a organisé une protestation en ligne contre l'OMC sur ces bases, au cours de laquelle il est parvenu à ralentir l'accès au site pendant plusieurs heures, suite à la participation de 452 000 internautes. En mars 2000, il a également invité ses sympathisants à bombarder de courriers électroniques 76 officiels américains dans le cadre d'une opération baptisée « *Resistance is Fertile* »[33], destinée à protester contre la banalisation des OGM aux Etats-Unis et dans le reste du monde. Le projet suivant des

[30] Ce slogan est le nom d'un projet multimédia lancé en janvier 1995 par les militants pro-zapatistes de Zapnet, et hébergé par l'université du Texas ; cf. http://www.actlab.utexas.edu/~zapatistas/info.html. La phrase fait (contre-)référence à la célèbre chanson de Gil Scott-Heron, « The Revolution will not be televised ».

[31] http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html.

[32] « Ethics of hactivism », http://www.sans.org/infosecFAQ/hackers/hacktivism2.htm.

[33] Ce slogan fait (contre-)référence à un morceau du *jazzman* Steve Coleman intitulé « Resistance is futile ».

Electrohippies consistait en une gigantesque opération de déni d'accès visant les grands noms du commerce électronique, qu'ils justifièrent en se comparant au Christ chassant les marchands du temple[34]. Cette action fut cependant annulée en raison du vote de défiance des sympathisants en ligne du groupe. Si le hacktivisme se veut une technique de protestation de masse, il peine donc encore à trouver son audience. Parmi les *hackers*, notamment, son usage demeure controversé. Ainsi le cDc a-t-il engagé une violente polémique avec les Electrohippies, en accusant ces derniers de rationaliser les actions de déni d'accès et donc de violer le Premier amendement de la Constitution américaine[35]. Le cDc différencie en fait le « hacktivisme » – qu'il pratique dans le cadre de son projet « *Hacktivismo* »[36] – du simple « (h)activisme » : « Le premier cherche à pallier les mauvaises conduites sur l'internet et les restrictions ou le manque d'accès à celui-ci, etc. ; le second cherche à faire du net un *medium* publicitaire ou un agent de transformation sociale sur le terrain à travers diverses actions de protestation »[37]. La liste de diffusion (*mailing list*) hacktivism.tao.ca, lancée à l'été 1999 et récemment rebaptisée hacktivism.openflows.org, témoigne également de la virulence des débats parcourant la « scène » sur les usages politiques du *hacking*, auxquels un « e-zine » est désormais consacré : thehacktivist.com.

Les seules causes susceptibles de rallier en masse les *hackers* sont en fait la promotion de la liberté de circulation de l'information dans le cyberespace et la défense de leurs confrères ayant maille à partir avec la justice de leur Etat. A l'occasion de l'affaire Altern, une coalition de milliers d'internautes et de centaines de webmestres (qui fermèrent leurs sites en signe de protestation) parvinrent ainsi à obtenir la réouverture de l'hébergeur gratuit et indépendant alors menacé par la justice. La défense de Kevin Mitnick ou celle d'Emmanuel Goldstein, rédacteur en chef de *2600. The Hacker Quarterly*[38], ont quant à elles constitué les causes les plus consensuelles de la « scène » de la fin des années 1990. Ces éléments suggèrent l'existence d'un véritable « communautarisme électronique » en son

---

[34] « DJNZ », cité dans « Ethics of hactivism », *op cit*.

[35] « To heck with hacktivism », *Salon.com*, 20 juillet 2000.

[36] Celui-ci est consacré à la défense de la liberté d'information sur l'internet et a été lancé en 1999, dans la foulée du Defcon, la réunion annuelle la plus courue des *hackers* ; cf. http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html ; le 4 juillet 2002, le cDc a présenté à la presse son nouveau programme « anti-censure », qui permet d'échanger des informations interdites en les dissimulant sous des images au format .GIF ; le programme est, depuis cette date, librement accessible sur le site du groupe ; cf. http://hacktivismo.com/news/modules.php?name=Content&pa=showpage&pid=12/.

[37] « Hacktivism in the cyberstreets », *AlterNet*, 30 mai 2000, disponible à l'adresse suivante : http://www.alternet.org/story.html?StoryID=9223.

[38] Revue phare de la « scène » *hacker*, qui diffusa les codes sources permettant de « craquer » des DVD sous Linux.

sein, conduisant ses membres à se mobiliser en priorité pour leurs confrères, sur fond d'éloges de l'ultralibéralisme communicationnel. Cet attachement passionnel des *hackers* à la liberté de circulation de l'information sur les réseaux les apparente au mouvement libertarien américain (LOADER : 2 ; FLICHY, 2001 : 208-212) et se trouve teinté d'un « technopopulisme » virulent. Ainsi l'Electronic Frontier Foundation[39] présente-t-elle sa mission :

> Imaginez un monde où la technologie nous aurait tous rendus capables d'échanger le savoir, les idées, les pensées, les humeurs, les mots et l'Art avec des amis, des inconnus et les générations futures. Ce monde est ici et maintenant, il est rendu possible du fait du réseau électronique – l'internet – qui a le pouvoir de tous nous connecter les uns aux autres. Et les développements futurs de la technologie vont nous permettre d'accéder à l'information et de communiquer avec les autres de manière plus puissante encore. Mais les gouvernements et les multinationales essaient de nous empêcher de communiquer librement par l'intermédiaire des nouvelles technologies, de la même manière qu'au Moyen-âge les puissants contrôlaient la production et la distribution des livres – ou même les brûlaient – parce qu'ils ne voulaient pas que le peuple lise. Ce n'est qu'en luttant pour nos droits à la liberté d'expression, quel que soit le *medium* – qu'il s'agisse de livres, de téléphones ou d'ordinateurs – que nous parviendrons à protéger et à améliorer la condition humaine.[40]

Malgré ce « technopopulisme » des *hackers* et de certains hacktivistes, la frontière entre « gendarmes » et « voleurs » est une ligne ténue, voire inexistante, dans le cyberespace. Ce dernier point est fondamental, puisqu'il suggère l'ambivalence du caractère « subversif » de la « scène », limitant encore un peu plus le potentiel du *hacking* en termes de contestation de l'ordre établi et de transformation sociale. Pour Tim Jordan et Paul Taylor, « à n'en pas douter, sa relation la plus importante à une autre communauté ou à un autre groupe, celle qui définit le mieux la communauté *hacker* tient au lien intime et antagonique qu'elle entretient avec l'industrie de la sécurité informatique (ISI) » (JORDAN & TAYLOR, 1998 : 770). Aucun autre groupe ne participerait aussi directement à la constitution de la communauté du *hack*. Les membres de l'ISI assimilent souvent les *hackers* à de la « vermine », à des « vandales électroniques », ou encore à « des gamins qui mettent une pièce d'un penny sur des rails pour voir si le train peut la plier, sans réaliser qu'ils risquent de le faire dérailler »[41]. Mais les frontières entre les deux communautés sont en fait loin d'être aussi étanches que ces propos le laissent entendre[42], comme le constate le *hacker* américain « Mofo » : « mon expérience m'a montré que les 'responsables' de systèmes et de réseaux s'enivrent des mêmes sentiments de puissance [*power trips*] [que les *hackers*] »

[39] Il s'agit là d'une organisation d'activisme en ligne plutôt que de hacktivisme au sens strict, dans la mesure où elle se cantonne à la défense de la liberté d'expression dans le cyberespace. Au fil des années, l'EFF a pourtant assuré la défense juridique de nombreux *hackers*, qui constituent l'essentiel de ses militants.

[40] http://www.eff.org/abouteff.html.

[41] Mike Jones, responsable de la section de sensibilisation à la sécurité, ministère du Commerce et de l'Industrie britannique, cité par JORDAN &TAYLOR, 1998 : 770.

[42] « Cutting to the chase: Hackers join forces with security firms to keep the world safe », *Boston Herald*, 18 janvier 2000.

(cité dans *ibid*). En outre, de nombreux *hackers* rêvent d'être recrutés par l'ISI et il suffit de consulter un site comme Attrition.org[43] pour constater que de nombreux *hacks* n'ont d'autre objectif que d'attirer l'attention des responsables d'un site donné sur ses failles en matière de sécurité, en vue d'obtenir un éventuel recrutement. Ainsi certains *hackers* n'hésitent-ils pas à laisser leur adresse électronique sur les pages qu'il défigurent, la virtuosité du *hack* et sa mise en relief de failles sécuritaires constituant le meilleur des *curriculum vitae* pour un jeune *hacker* en quête d'emploi. On imagine mal un voleur se voir proposer un emploi de policier du fait du brio de ses larcins, ou « téléphoner à une banque pour se plaindre du laxisme en termes de sécurité » (*ibid* : 772), mais c'est bien ce qui se produit régulièrement dans le cyberespace, où les « gendarmes » sont souvent d'anciens « voleurs ». Même les *hackers* les plus fameux n'ont pas échappé aux attraits financiers de l'ISI. Eric Bloodaxe, alias Chris Goggans, fondateur de la Legion of Doom (LoD), a par exemple participé à la fondation d'une firme de sécurité informatique, Comsec, avant de devenir ingénieur dans le domaine de la sécurité des réseaux pour la compagnie WheelGroup. Les membres du Cult of the Dead Cow, qui sont pourtant les *hackers* les plus radicaux de la « scène », avouent eux-mêmes qu'ils travaillent pour l'ISI, et John Draper, alias « Cap'n Crunch », développe aujourd'hui des *firewalls* en partenariat avec la société ShopIP. Au sein des entreprises de sécurité informatique, les compétences des *hackers* sont souvent valorisées dans la mesure où elles permettent d'identifier rapidement un problème ou de répondre à une attaque. IBM elle-même recrute parfois des *hackers* pour attaquer certains systèmes informatiques. De nombreux services de renseignement ont également recours aux compétences de leurs adversaires potentiels. Tous ces éléments suggèrent l'ambivalence des relations entre agents de la surveillance et fauteurs de troubles dans le cyberespace, rappelant l'ambiguïté des liens unissant *hackers* et multinationales dans les romans de Gibson. Ni parfait gendarme ni complet voleur, le *hacker* est un joueur invétéré, un étudiant attardé et un provocateur enragé. De là l'irréductibilité du *hack* au politique, que celui-ci soit (temporairement) mis au service de la surveillance ou, au contraire, de la « provocation permanente » du pouvoir dont parle Michel Foucault (FOUCAULT, 1982 : 222).

[43] Le site, monté par d'ex-*hackers* passés à l'ISI, archive les pages « défigurées » par des *hackers* du monde entier : http://www.attrition.org.

Contribuant à l'émergence d'un espace public international, l'internet participe également à la construction des identités contemporaines, que celles-ci trouvent leurs origines en ou hors ligne. Les « communautés imaginées » *offline* se réinventent dans le cyberespace, où sont parallèlement apparues des « communautés virtuelles » dont les membres se fréquentent parfois hors ligne. Dans ces conditions, comme le note Sue Gunawardena, « le cyberespace constitue un site idéal pour ré-imaginer sa patrie [*homeland*] et concrétiser les abstractions du mythe nationaliste » (GUNAWARDENA, 2000 : 272). Les nouvelles technologies de l'information renforcent notamment les liens entre les communautés transnationales de migrants et leur société d'origine et offrent la possibilité à tout individu disposant d'un capital techno-social minimal de se muer en entrepreneur identitaire en ouvrant un site d'information *sur* ou *pour* sa communauté.

En étendant ses ramifications au cyberespace, le nationalisme a entamé une véritable révolution copernicienne, dans la mesure où ce discours a été conçu pour un monde westphalien, dominé par le couple moderne de l'Etat souverain et du territoire borné, et non pour un réseau déterritorialisé tel que le *world wide web*. Quelle formes prennent alors les manifestations du nationalisme en ligne et dans quelle mesure celles-ci suggèrent-elles l'avènement d'un « post-nationalisme », c'est-à-dire d'un nouveau mode de subjectivation politique ? L'essor du cyberespace induit-il l'affaiblissement des modes de gouvernance stato-centrés, où contribue-t-il au contraire à l'affermissement de l'action étatique et à la résilience des référents stato-centrés parmi les entrepreneurs identitaires occupés à y imiter l'Etat ? Nous proposerons ici quelques premiers éléments de réponse à ces questions à partir de l'étude des relais en ligne de deux mouvements nationalistes d'Asie du Sud : celui des sikhs du Pendjab (à l'origine du mouvement « khalistani »[44]) et celui des Mohajirs du Sind (animé par le Mohajir Qaumi Movement[45]). Nous nous pencherons également sur

[44] Le mouvement séparatiste sikh a émergé au Pendjab indien après l'opération Bluestar de juin 1984, au cours de laquelle l'armée indienne prit d'assaut le Temple d'Or d'Amritsar, où s'étaient retranchés Sant Jarnail Singh Bhindranwale et ses partisans. Ce mouvement sécessionniste armé, œuvrant à la création d'un Etat souverain sikh (le « Khalistan », ou « pays des purs »), a été militairement défait dès 1992, suite à une répression féroce. Il demeure pourtant puissant dans la diaspora sikhe, où il s'est greffé à ses « politiques de reconnaissance » dans ses Etats d'accueil. A ce sujet, nous renvoyons à notre propre travail : GAYER, 2000.

[45] Le MQM, fondé à Karachi en 1984 par Altaf Hussain, défend les intérêts des descendants des musulmans indiens qui émigrèrent au Pakistan après la Partition de 1947. Le parti, dirigé de Londres depuis le début des années 1990 suite à l'exil de son leader, disposerait – aux dires de ses dirigeants – d'une trentaine de bureaux aux Etats-Unis, de trois au Canada et en Afrique du Sud, d'une dizaine au Royaume-Uni, d'un en Belgique, en Hollande, au Japon, en Australie, en Arabie saoudite, aux Emirats arabes unis et au Koweït.

l'essor du hacktivisme anti-indien, dont les principaux acteurs se trouvent au Pakistan mais dont les relais s'étendent de la Nouvelle-Zélande au Brésil.

Nations en ligne et Etats virtuels

La question des rapports entre transformation des systèmes d'information et construction du nationalisme, qui mobilise les politologues depuis les années 1950, a fait l'objet de nombreuses controverses. La plus fameuse reste sans doute celle qui opposa Ernest Gellner à Karl Deutsch, le premier contestant la validité du modèle cybernétique du second (DEUTSCH, 1953) en insistant sur le fait que les médias modernes diffusent moins le nationalisme qu'ils ne le façonnent eux-mêmes (GELLNER, 1983 : 126-127). Plus récemment, Jean-Pierre Bacot a montré que les magazines illustrés européens ont « porté » autant que « construit » les identités nationales dans la seconde moitié du XIXe siècle. Les gravures reproduites par ces publications auraient notamment joué un rôle décisif en « [installant] dans les esprits des représentations de l'autre, de l'ami et de l'ennemi, un univers de croyances provisoires, sans cesse reconfigurées » (BACOT, 2001 : 277). L'essor de l'internet pose cependant des problèmes spécifiques aux théoriciens du nationalisme, qui se trouvent ici en présence d'un média électronique interactif et multifonctionnel.

Ainsi que le note Haleh Nazeri dans son étude sur les « cyber-communautés imaginées » iraniennes, « de nombreuses communautés diasporiques se sont emparées de l'internet pour maintenir leurs connections avec leurs compatriotes dispersés à travers le monde » (NAZERI, 1996 : 158). De nombreuses nations d'abord imaginées hors ligne se réinventeraient ainsi dans le cyberespace, qui favorise l'avènement d'espaces de discussion autogérés, consacrés à la politique, à l'adaptation des « traditions » à la modernité, à la sexualité, à la musique, au cinéma, à la gastronomie, etc. L'internet permet également l'épanouissement de relations sociales directement orientées vers le monde réel, du transfert de capitaux aux alliances matrimoniales. Comme le relève Haleh Nazeri, de nombreux exilés trouvent dans l'internet un moyen de nouer des relations d'amitié, d'affermir leur identité et de se convaincre de l'existence de compatriotes aux intérêts similaires et également désireux de ne pas renoncer à leur culture d'origine. L'internet constituerait un outil particulièrement attrayant pour ces populations diasporiques, dans la mesure où il contribue au développement de liens transnationaux « plus immédiats, plus libres, plus intenses et plus efficaces » (VERHULST, 1999 : 30-31, cité par ROBINS, 2001 : 26). L'internet permet

également à ces populations d'accéder à des médias « ciblés », destinés à des publics spécialisés et « homogènes », qui, pour certains auteurs, triompheraient aujourd'hui des médias de masse (ELKINS, 1997).

Cette réflexion sur les relais cyberspaciaux des processus de construction identitaire est pourtant trop vaste pour que ne fassions que l'effleurer, et nous nous concentrerons ici sur les ramifications cyberspatiales de deux mouvements « nationalitaires » du sous-continent indien, dans la mesure où nous souhaitons éviter de nous perdre dans une approche par trop générale des politiques identitaires sur l'internet, mais également parce que nos travaux de terrain nous ont conduit à fréquenter régulièrement cette région du monde et ces mouvements contestataires[46].

Tous les groupes nationalistes d'Asie du Sud sont aujourd'hui actifs dans le cyberespace. La plupart ont ouvert des sites internet au milieu des années 1990, pour répondre à trois objectifs : (1) informer leurs militants et leurs sympathisants des décisions du *leadership* et des actions politiques futures ; (2) promouvoir la cause du mouvement auprès de la « communauté internationale » ; (3) récolter des fonds auprès de leur diaspora.

Le Mohajir Qaumi Movement (MQM) a sans aucun doute été le plus habile dans son utilisation de l'internet comme interface entre sa direction et sa base. Le site de ce parti pakistanais aux activités mondiales est pour le moins remarquable. Celui-ci a été développé par des informaticiens mohajirs des Etats-Unis puis « rapatrié » en Grande-Bretagne au milieu des années 1990, et il permet aux militants et aux sympathisants du parti de s'informer en temps réel de la situation politique à Karachi et des positions du *leadership*, au Pakistan comme à l'étranger. Il est en outre possible de contacter le parti *via* l'e-mail indiqué sur le site. En bref, mqm.org est devenu en quelques années le centre névralgique du dispositif d'internationalisation du parti, passé maître dans l'utilisation des technologies de l'information[47]. Le site a vocation à servir de diffuseur et de récepteur d'information, à destination et en provenance de la « communauté internationale » mais aussi, et surtout, des Mohajirs eux-mêmes, puisqu'une large part des articles, discours, poèmes ou chansons disponibles sur le site sont en ourdou. Ainsi le site comporte-t-il onze sections principales : (1) informations ; (2) biographie/photographies/articles/discours d'Altaf Hussain ; (3) accès

[46] Auxquels nous avons consacré notre thèse, intitulée « L'international de l'identitaire. Origines et répercussions internationales des politiques identitaires sikhe et mohajir », que nous soutiendrons à l'IEP de Paris, courant 2003.

[47] Altaf Hussain aime ainsi à s'entretenir avec ses militants du monde entier par conférence téléphonique, *via* un ingénieux système de téléphones portables connectés à des amplificateurs. Le fax est également un instrument de prédilection du MQM et le « Media Centre » du parti à Karachi n'en compte pas moins de six.

aux unes des principaux journaux pakistanais ; (4) informations en ourdou ; (5) chansons du MQM ; (6) photographies ; (7) manifeste du parti ; (8) cercles d'études ; (9) raids et arrestations des militants au Pakistan ; (10) services philanthropiques ; (11) poésie. Outre ces entrées, on peut trouver sur le site le texte des résolutions récemment adoptées par le parti ainsi que des liens vers divers sites d'information ou articles[48]. En période de ramadan, le site offre également une plate-forme pour collecter les dons religieux (*zakat*, *fitrah*, *sadaqa*, etc.) qui seront envoyés au Pakistan pour financer les activités de la fondation philanthropique du parti, la *Khidmat-e-Khalq Foundation* (KKF), ou encore pour appuyer financièrement les familles des *shahids* (martyrs) du parti.

La dimension antagonique de ce site transparaît à plusieurs niveaux. Sur la page d'accueil, le MQM propose un dossier consacré à la plus fameuse agence de renseignement pakistanaise, l'ISI (Inter Services Intelligence), dont les agents se trouvent accusés de constituer un « Etat dans l'Etat », un « gouvernement invisible », etc. Sur cette même page, le MQM présente son programme comme « une campagne contre la domination des féodaux », révélant là son populisme virulent. Le MQM y souligne également le soutien qu'il a récemment reçu de la part des parlementaires britanniques, qui ont appelé les autorités pakistanaises à « ne pas répéter l'opération armée [de 1992] contre le MQM »[49]. Le parti attend en fait un « effet de boomerang » de tels soutiens extérieurs (KECK & SIKKINK, 1998 : 12), l'appui de la « communauté internationale » devant lui permettre de se libérer de certaines contraintes au Pakistan (arrestation de ses militants et limitation de ses activités politiques après le coup d'Etat de 1999). Le soutien apporté par le parti à la campagne anti-terroriste américaine, longuement détaillé sur son site internet, s'inscrit également dans le cadre de cette « diplomatie identitaire » qui vise à médiatiser les activités du « troisième parti du pays » et à redorer son blason, entaché par de nombreuses années de lutte armée entre ses militants et les diverses forces en présence à Karachi[50]. Ainsi la confrontation entre la direction exilée du MQM et l'*establishment* pakistanais qu'elle combat (composé des « féodaux », des « capitalistes » et de l'armée) se trouve-t-elle euphémisée sur le site du parti, qui a autant vertu à constituer une interface entre ses militants du Pakistan et de l'étranger qu'entre sa direction et la « communauté internationale ». La prudence rhétorique y est donc de rigueur et

[48] Ainsi trouve-t-on sur le site un lien vers un article consacré à la fameuse militante du Front de libération de la Palestine (FPLP), Leila Khaled, ainsi que vers un article de Robert D. Kaplan, « The lawless frontier », reprenant, à partir de l'exemple pakistanais, les thèses désormais bien connues de l'auteur sur la « nouvelle anarchie » menaçant, selon lui, l'ordre mondial depuis la fin de la guerre froide.

[49] Cf. http://www.mqm.org/English-News/Dec-2001/hocuk011205.htm.

[50] Les militants mohajirs ont d'abord affronté les partis religieux implantés sur les campus universitaires du Sind, puis les barons de la drogue et la mafia des transporteurs pathaans, les organisations nationalistes sindhies et enfin l'armée pendjabie.

aucune trace de séparatisme ou de propension à la violence ne peut y être décelée, cette modération langagière contrastant fortement avec les propos tenus devant nous par les militants de base et certains cadres du parti, au Pakistan comme à l'étranger. L'un de ces militants nous avait ainsi déclaré, en avril 2000, à Washington : « Peut-être que nous pourrions créer la société utopique que tout le monde cherche… Exactement comme ici [aux Etats-Unis] : un pays parfait. C'est possible. Si Altaf Hussain en appelle à la foule, alors il peut le faire, il en a le pouvoir, les gens l'écoutent toujours. Dans ces conditions [d'indépendance], Karachi connaîtra un tel taux de croissance que, de là, nous contrôlerons toute l'Asie du Sud. La ville connaîtra le plein-emploi et toutes les compagnies informatiques viendront s'installer dans la région. Ce ne sera pas du gâteau mais une fois que nous aurons notre Etat, nous nous entendrons bien avec tous les Etats alentours. Mais pour y parvenir, nous devrons utiliser la force. Car nous ne pourrons jamais y parvenir sans faire usage de la violence. C'est dur, mais parfois, quand voulez vraiment quelque chose, ou bien vous la fermez, ou bien vous allez jusqu'au bout. Même si vous devez tuer quelques personnes. Parce que si vous voulez gagner quelque chose, alors vous devez aussi perdre quelque chose ».

L'irénisme médiatique du MQM, qui contraste avec sa brutalité sur le terrain pakistanais, inquiète Islamabad, qui craint de voir le parti d'Altaf Hussain accéder à la respectabilité internationale. Les autorités pakistanaises ont donc cherché à contrer cette diplomatie identitaire par le biais d'une campagne de diffamation télématique. Le site du gouvernement pakistanais a ainsi publié la liste des atrocités attribuées au MQM ainsi que celle des armes que les forces de sécurité auraient retrouvées aux domiciles de militants mohajirs[51]. En réponse, le MQM a menacé le gouvernement pakistanais de poursuites si des matériaux jugés « offensants pour le parti » n'étaient pas retirés du site officiel du gouvernement.

Si le conflit entre le MQM et Islamabad a donc bien été étendu au cyberespace ces dernières années, celui-ci y demeure au stade de la guerre des mots et il est peu probable qu'il dérape vers des activités de « cyberguérilla », du fait de son exposition au regard de tous.

Les militants séparatistes sikhs font également une utilisation intense et multiforme de l'internet. Comme l'a repéré Sue Gunawardena, la présence sikhe dans le cyberespace s'organise autour de trois types de sites : (1) des sites « généralistes », tels que Sikhnet

[51] Cf. http://www.fas.org/irp/world/para/docs/mqm-factsheet.htm ; http://www.fas.org/irp/world/para/docs/yearwise_detail_mqm.htm ; on notera également sur http://www.fas.org/irp/world/para/docs/mqm_factsheet.htm#1 l'équation opérée par le gouvernement pakistanais entre le MQM et les nazis.

[http://www.sikhnet.com], proposant des forums et des espace de discussion en temps réel (*chat rooms*), des nouvelles de la diaspora et du sous-continent, etc. ; (2) des sites religieux, tels que The Sikhism Homepage [http://www.sikhs.org], qui se consacrent à la dissémination d'informations au sujet du sikhisme, à destination du *Panth*[52] comme des non-initiés ; (3) des sites politiques, tels que Khalistan.net [http://www.khalistan.net], revendiquant la création d'un Etat souverain sikh au Pendjab indien (le « Khalistan », ou « pays des purs ») (GUNAWARDENA, 2001 : 274). C'est cette dernière catégorie de sites qui nous intéresse ici. Force est d'abord de constater leur nombre et leur concurrence, témoignant du syndrome de scissiparité qui fragilise le mouvement khalistani en comme hors ligne. A la différence du mouvement mohajir, animé par un parti unique[53] dirigé d'une main de fer par un leader charismatique[54], la mouvance khalistanie est caractérisée par son éclatement en divers groupes eux-mêmes divisés en factions adverses, dont n'a jamais émergé de figure consensuelle. La présence des nationalistes sikhs et mohajirs sur l'internet reproduit donc, en ligne, les modes d'organisation et les lignes de fracture qui les caractérisent hors ligne. Ainsi le « cyberkhalistanisme » s'organise-t-il autour de sites en compétition pour le monopole de la parole légitime sur la nation sikhe et sur son territoire. Malgré leur opposition apparente, ces sites présentent pourtant de nombreux points communs. Tous s'organisent autour des trois objectifs définis plus haut : *communication*, *médiatisation* et *financement*, auxquels s'ajoutent parfois ici un projet d'*imitation de l'Etat*. Celui-ci consiste, pour les cyber-nationalistes sikhs, à s'approprier les attributs symboliques de l'Etat (monnaie, drapeau, hymne, territoire cartographié) et à les répliquer en ligne de la manière la plus convaincante possible, afin de renforcer la visibilité et la crédibilité de leurs organisations, tant auprès du *Panth* que de la « communauté internationale ».

Depuis sa genèse dans les années 1940 au Pendjab, la rhétorique khalistanie s'est articulée autour de la revendication d'un autre « pays des purs », envisagé comme un Etat-tampon entre l'« Hindoustan » et le Pakistan. Dans les années 1980, le Dr. Jagjit Singh Chauhan chercha à donner corps à ce projet en fondant un gouvernement en exil du Khalistan à Londres. Le Khalistan Council imita alors les fonctions régaliennes de l'Etat, notamment en diffusant au Pendjab des passeports et des billets du Khalistan, fabriqués au

[52] Ce terme signifie littéralement « la voie » et, par extension, la communauté sikhe.

[53] Au début des années 1990, une partie des cadres du MQM ont fait scission pour former le MQM Haqiqi (« véritable »), mais celui-ci n'a jamais percé politiquement, du fait de son étroite association aux services de sécurité. Les affrontements entre le MQM (Altaf) et le MQM (Haqiqi) ont néanmoins fait des centaines de morts à Karachi depuis 1992.

[54] Ce charisme est de nature mystique, Altaf Hussain étant considéré comme un *pir* (chef de confrérie soufie) par ses militants. Oscar Verkaaik estime cependant que cet emprunt au soufisme est ironique et que la véritable source de la popularité d'Altaf Hussain est sa « banalité », qui permet à chaque mohajir de s'identifier à lui (VERKAAIK, 1999).

Canada. Chauhan s'autoproclama même Président du gouvernement khalistani en exil et ouvrit un « consulat » à Londres, la Khalistan House. Il ne s'agissait pourtant pas de fonder un *véritable* Etat khalistani : « les gens mythifient la conception des passeports et des billets de banque, mais dès que vous comprenez qu'en fait ce n'est rien du tout, alors vous pouvez le faire comme ça, en un claquement de doigts ; mais bien sûr, tout cela était symbolique »[55]. Cette entreprise de *state-building* virtuel visait donc à démythifier le puissant Etat indien en attentant symboliquement à sa souveraineté, ainsi qu'à conforter la légitimité de Chauhan et de son organisation auprès du *Panth* comme de la « communauté internationale », plutôt qu'à mettre sur pied un véritable gouvernement en exil du Pendjab. Cette imitation provocante de l'Etat, destinée à légitimer les nationalistes sikhs de l'extérieur, a récemment été étendue au cyberespace ; alors qu'en 1994 il existait seulement deux sites khalistanis, on en dénombre aujourd'hui plus de six cents (AXEL, 2001 : 142). Le plus célèbre d'entre eux, khalistan.net, est animé par un ancien chercheur en génétique moléculaire, le Dr. Gurmit Singh Aulakh, et l'on s'y trouvait, jusque récemment, accueilli par les mots « *Welcome to the sovereign cyberspace of Khalistan !* », auxquels s'est depuis peu substitué le slogan « *Khalistan, the new global reality* », apposé sur une carte du monde où le Pendjab se trouve désigné d'une flèche. Sous ce titre, on découvre une série de photographies et de reproductions de tableaux représentant le premier et le dernier gourous sikhs (Nanak et Gobind Singh), une page du *Guru Granth Sahib*[56], l'Akal Takht[57], le Temple d'Or, le *Nishan Sahib*[58], Sant Jarnail Singh Bhindranwale, une carte du Khalistan, ainsi que le Dr. Aulakh occupé à ratifier l'entrée de son organisation, le Council of Khalistan, au sein de l'Unrepresented Nations and Peoples Organisation (UNPO)[59].

Imiter l'Etat territorial dans le cyberespace déterritorialisé peut sembler paradoxal et voué à l'échec. En se retranchant dans les réseaux électroniques après avoir échoué sur le terrain pendjabi, le mouvement khalistani a pourtant trouvé une nouvelle jeunesse. L'Etat

[55] Entretien avec le Dr. Jagjit Singh Chauhan, Londres, 16 juillet 1999.

[56] Principal texte sacré sikh, rassemblant les écrits des gourous sikhs et compilé par le dernier gourou, Gobind Singh, au XVIIIe siècle.

[57] Le « Trône de l'Immortel », construit par le sixième gourou, Hargobind, défiait l'autorité moghole et symbolise la dimension temporelle du pouvoir divin (*miri*) alors que le Temple d'Or proprement dit (*Harmandir Sahib*) symbolise sa dimension spirituelle (*piri*). Le Takht fut détruit à l'occasion de l'opération Bluestar de juin 1984 ; reconstruit par le gouvernement indien, il fut à nouveau rasé par le *sangat* (assemblée des croyants sikhs) puis reconstruit par ses membres dans le cadre du *seva* (service à la communauté). Les nationalistes sikhs présentent l'Akal Takht comme le siège historique de la souveraineté sikhe (le *Halemi Raj*).

[58] Drapeau triangulaire safran, frappé du *khanda*, symbole du *Panth*.

[59] Le Council of Khalistan fut admis au sein de l'UNPO en 1993 mais il en fut exclu peu après, sa représentativité s'étant trouvée mise en doute et la personnalité d'Aulakh lui ayant probablement aliéné de nombreux membres de l'organisation, acquis à des méthodes moins bruyantes.

territorial khalistani, qui n'a jamais été sérieusement théorisé, s'efface dans le « cyberkhalistanisme ». Il y devient un simple *mantra*, une formule magique reconnue comme telle, unissant les fidèles par-delà les frontières. Ainsi, pour l'ex-porte-parole de la Khalistan Commando Force à Londres, qui s'autodéfinit comme un « *cyber-panjabi* »,

> les cartes ne sont pas importantes pour notre mouvement, parce que quand vous vous focalisez là-dessus, vous devenez une puissance hégémonique et impérialiste. L'histoire est de notre côté. Mais on ne peut construire les identités sur du vent : il faut retourner à sa culture, à son héritage, à ses racines, et y puiser les matériaux nécessaires et, d'une certaine manière, les refaçonner et leur donner une nouvelle interprétation (…). L'Etat hégémonique est menacé, parce que vous ne pouvez plus supprimer des peuples aujourd'hui. Mais avant d'inventer un nouveau type d'Etat, nous devons adopter un nouvel *état d'esprit*. [60]

Ce militant a cherché à mettre ce discours en pratique en fondant une ONG basée à Southall[61], le Panjabi Centre, qui s'est récemment doté d'un site internet et qui, depuis mai 2002, anime DesiRadio, la première radio pendjabie du monde à émettre 7 jours sur 7 et 24 heures sur 24. La brochure publicitaire de l'ONG présente un « *Panjab* » seulement délimité par les « cinq rivières » d'où la province tire son nom, témoignant d'un dépassement explicite des frontières étatiques et de l'invention d'un nouveau *terroir* pendjabi, interculturel et transfrontalier. Ce *Panjab* imaginaire a vertu à rapprocher Pendjabis sikhs, hindous et musulmans, dans le sous-continent et surtout en diaspora, ce processus de réconciliation nationale étant destiné à refermer les plaies de la Partition et à soutenir les efforts du *lobby* « Panjabis in Britain » animé par la même équipe d'anciens khalistanis reconvertis en « lobbyistes ethniques ».

L'imitation paradoxale ou le dépassement explicite de l'Etat dans le cyberespace ont tous deux vertu à renforcer des liens sociaux, locaux et translocaux (MANDAVILLE, 2001), plutôt qu'à façonner des structures politiques effectives. « Cyberkhalistanisme » et « pan-pendjabisme » participent à la construction d'un espace d'*appartenance* plutôt que de *gouvernance* qui contribue à rapprocher les sikhs du monde entier. De fait, pour les jeunes militants khalistanis de la diaspora, l'internet constitue l'accès principal à la littérature nationaliste et à la mémoire des évènements de 1984. Politisés par l'entremise du *world wide web*, ces jeunes gens y ont trouvé un espace d'identification complémentaire à celui de leur milieu local, qui n'est pas sans rappeler « l'oummah virtuelle » étudiée par Olivier Roy (ROY, 2001). Cet espace essentiellement symbolique (GUNAWARDENA, 2001 : 311) est aujourd'hui imaginé au-delà du territoire, dans la mesure où, comme le fait remarquer un jeune militant khalistani de Birmingham, « pour beaucoup de sikhs orthodoxes, le Khalistan

[60] Entretien, Londres, 22 juillet 1999.

[61] Quartier pendjabi de la banlieue ouest de Londres.

c'est le monde entier, et dans la mesure ou les sikhs sont dispersés dans le monde entier, et bien la *sikhi* [identité sikhe] aussi »[62].

L'Etat virtuel proposé par les « cyber-khalistanis » et le terroir imaginaire inventé par les « pan-pendjabistes » cherchent donc à rendre plus proche et plus concret une « patrie » (*watan*) aux contours géographiques flous[63], dont de nombreux sikhs se trouvent éloignés et qu'ils n'ont même parfois jamais visitée. Ainsi l'Etat virtuel proposé par les « cyber-khalistanis » contribue-t-il à donner forme à ce *Panjab* qui, hors ligne, apparaît trop abstrait auprès de nombreux sikhs. Reste qu'en cherchant à concrétiser un espace territorial abstrait en le matérialisant symboliquement dans le cyberespace, ces entrepreneurs identitaires sont sortis du paradigme nationaliste et contribuent à inventer un espace d'appartenance à la fois plus tangible (car visualisable de tout point de la Terre et à tout instant) et plus flou (car constitué par des symboles textuels et iconographiques plutôt que par des frontières) que ne l'était le territoire. Bien qu'ils se situent explicitement dans un cadre post-national, les « pan-pendjabistes » demeurent eux aussi sous l'emprise de l'Etat. Ils se cherchent un nouvel « état d'esprit » post-westphalien mais concentrent leurs activités de lobbying sur des cibles étatiques et fonctionnent rarement en réseaux transnationaux, chaque organisation travaillant généralement de manière autonome à l'échelle d'un pays, d'une ville et plus souvent encore d'un quartier. Le « post-nationalisme » sikh demeure donc balbutiant, ses acteurs peinant à échapper à l'emprise de l'Etat et du local, tout en se trouvant contraints à un grand écart permanent entre l'universel et le particulier, entre adhésion aux nouvelles utopies planétaires et réinvention de la différence.

Les usages de l'internet par les groupes nationalistes contemporains dessinent une « géographie des sentiments » qui concrétise le rapport social et politique des individus à leurs espaces de référence dans le monde réel tout en brouillant les contours proprement géographiques de ces nouvelles spatialités. Ainsi, cette autre « hallucination consensuelle » qu'est la nation se trouve-t-elle réimaginée dans le croisement de nouvelles politiques nationalitaires en et hors ligne, dont les acteurs perpétuent parfois le discours nationaliste propre au monde westphalien sans avoir conscience de le travestir. Dans les faits, l'effort de crédibilisation des « communautés imaginées » dans le cyberespace aboutit à l'apparition de

[62] Entretien, Southall, 18 juillet 1999.

[63] La délimitation du Pendjab est floue depuis l'époque moghole. La province tire en effet son nom des cinq rivières qui la parcourent mais le tracé de ses frontières a sans cesse évolué, au cours de la période moghole, sous le règne de Ranjit Singh puis à l'époque coloniale, au moment de la Partition (à l'occasion de laquelle elle se trouva partagée entre l'Inde et le Pakistan) et jusqu'en 1966, date à laquelle fut créée la province indienne du Pendjab, à majorité sikhe.

nouveaux espaces de référence dans le monde réel, à la fois en-deçà et au-delà du territoire, comme le suggère la notion de « translocalité » (MANDAVILLE, 2001).

Dans la perspective de la « nouvelle géographie », loin de s'opposer aux forces « globalisantes » du marché, ce « retour du local » en procéderait et lui répondrait, en vertu des « conséquences locales d'un besoin de plus grande intégration de sites décentralisés » (CLARKE & GOETZ, 1993). Ainsi se dessineraient les contours d'une « économie d'archipel » (VELTZ, 1996), tissant une vaste toile mondiale reliant les zones les plus dynamiques de la planète, notamment les grandes « villes globales » (SASSEN, 1991 ; KING, 1990), et reléguant au déclin les périphéries moins productives, à l'extérieur comme à l'intérieur du système. Au-delà de son caractère un peu suranné, ressuscitant sans grand discernement les thèses dépendantistes, cette approche a le mérite d'insister sur un point crucial : dans certains cas, la résurgence du « local » et la réinvention des différences s'opèrent dans le cadre d'un processus transnational d'*ouverture* vers le mondial plutôt que de *repli* vis-à-vis de forces menaçantes, c'est-à-dire d'*extra-* plutôt que d'*intro*version. L'essor de l'internet accompagne ce processus d'« extension » (*stretching*) des relations sociales (HOLMES, 1997: 5-6 ; LYON, 1997 : 24). Dans cette logique, « les rationalités politiques du localisme ne sont pas basées exclusivement sur l'esprit de privatisation (*privatism*) ou sur des valeurs communautaires ou même sur des logiques de spatialisation (*locational logics*) ; elles incluent également l'instrumentalisation du localisme comme stratégie politique pour contourner ou remplacer les structures dépassées des bureaucraties centrales » (CLARKE & GOETZ, 1993 : 5). Ainsi, la prétendue « tribalisation » de Karachi au début des années 1990 a-t-elle en partie relevé d'un désir d'intégration à l'espace transnational des flux économiques et financiers et d'une lassitude des entrepreneurs locaux à l'égard d'un pouvoir central considéré comme un frein à ce projet. Dans la même logique, le nationalisme sikh, cristallisé dans les années 1980, témoigne moins de l'essor global du fondamentalisme religieux que du désir des sujets politiques sikhs, en Inde et surtout en diaspora, de goûter aux délices conjugués de la souveraineté *et* de la transnationalité. Ainsi, pour un jeune avocat khalistani basé à New York :

> Dans les circonstances présentes, les fermiers sikhs ne peuvent pas vendre leurs récoltes hors de l'Inde. Mais s'ils se séparent de l'Inde, le monde entier devient leur marché… D'un seul coup, le Pendjab, cette région enclavée en Inde, devient le Pendjab, un Etat-nation qui fait partie intégrante de la communauté internationale. A présent, le Pendjab ne fait pas partie de la communauté internationale, il fait partie de la communauté nationale indienne. Maintenant, si nous avions un Etat séparé sikh, et bien d'un seul coup le Pendjab se retrouverait projeté sur la scène mondiale, et cela aurait de nombreux avantages pour bien des Pendjabis : cela nous permettrait de préserver notre langue, nos chansons, nos danses et plus généralement notre culture.[64]

[64] Entretien, New York, 12 avril 2000.

La guerre électronique aura-t-elle lieu ?

Au-delà des groupes nationalistes maniant l'internet à des fins de médiatisation, de financement et de construction identitaire, l'Asie du Sud a également vu se développer ces dernières années un hacktivisme anti-indien virulent, qui se greffe au conflit inter-étatique indo-pakistanais mais qui ne s'y trouve pas entièrement réductible. La plupart de ces groupes de *hackers* et de *script-kiddies* sont apparus depuis les essais nucléaires indiens de 1998. Le plus actif d'entre eux, GForce Pakistan, se compose de huit membres de nationalité pakistanaise, étudiants ou informaticiens. Ceux-ci se consacrent à la « défiguration » de sites indiens en vue d'attirer l'attention de l'opinion publique internationale sur « le massacre d'innocents (…) par les Indiens et les Israéliens », au Cachemire et en Palestine[65]. Depuis un an, le groupe compte plus de 200 sites piratés à son actif. Les jeunes *hackers* pakistanais n'ont pas épargné leurs propres autorités[66] et s'en sont également pris à des sites gouvernementaux américains. Leur principale cible demeure pourtant les sites indiens fortement médiatisés. En s'attaquant aux pages d'accueil de sites d'information tels que celui de la chaîne *Zee News* ou du magazine *India Today*, et en menaçant les sites liés au programme nucléaire indien d'attaques imminentes, les membres de GForce ont acquis un profil médiatique sans précédent. Ils ne sont pourtant pas les seules figures du hacktivisme anti-indien. D'autres groupes ont fait leur apparition ces dernières années, tels les Silver Lords (rassemblant *script-kiddies* pakistanais et brésiliens[67]), le Harkat-ul Mos, les Pakistan Hackerz ou le groupe Kill India. La multiplication des activités de ces jeunes hacktivistes[68] inquiète les autorités et les médias indiens, qui soupçonnent les services de renseignement pakistanais d'être impliqués dans ce « cyberjihad »[69] prétendument animé par des « islamistes » pakistanais et des « mercenaires » brésiliens[70]. Ce discours relève en fait du mythe plutôt que de la réalité. Comme le note Dorothy Denning, le hacktivisme privé

---

[65] http://www.srijith.net/indiacracked/interviews/gforce.shtml.

[66] A l'occasion du coup d'état militaire de 1999, les jeunes *hackers* piratèrent la page du gouvernement pakistanais pour la remplacer par une photographie des putschistes accompagnée d'un message de félicitations.

[67] Cf. l'interview des Silver Lords à l'adresse suivante : http://ttj.virtualave.net/interview_with_SilverLords.html.

[68] 131 sites indiens ont été piratés en 2000 et les estimations pour 2001 s'élèvent à 650 au moins. En avril 2001, les Silver Lords ont défiguré 23 sites indiens en six jours. Le regain de tension entre l'Inde et le Pakistan, suite à l'attentat contre le Parlement indien du 13 décembre 2001, s'est également traduit par une vague d'attaques, le groupe WFD ayant ainsi défiguré 20 sites le 22 décembre. A ce sujet, cf. le site « Project India Cracked », à l'adresse suivante : http://www.srijith.net/indiacracked/index.shtml.

[69] « Cyberjihad pakistanais contre l'Inde », *Libération*, 11 mai 2001.

[70] « Silver Lords lead record anti-India hacking spree », *Hindustan Times*, 27 avril 2001.

est souvent soupçonné de connivences gouvernementales mais celles-ci sont rarement avérées (DENNING, 2001). Les rares interviews disponibles des membres de GForce ou des Silver Lords suggèrent qu'il s'agit essentiellement d'adolescents pratiquant le *hack* par conviction politique (plutôt que religieuse), par désir de reconnaissance de la part de la « scène » et surtout par amusement. D'un site défiguré à l'autre, les Silver Lords peuvent ainsi laisser derrière eux un texte dénonçant la politique indienne au Cachemire aussi bien que les paroles d'une chanson de *hard-rock* ou une image tirée d'un *hentai* (*manga* pornographique)[71]. Ce serait donc faire preuve d'une imagination par trop débordante que de voir ici la patte de l'ISI, l'agence de renseignement pakistanaise. Dans le sous-continent indien comme ailleurs, les cyberconflits interétatiques demeurent de l'ordre du fantasme et ces attaques privées sont essentiellement d'ordre symbolique et ludique. En se banalisant, il est également probable qu'elles se trouveront moins médiatisées. On peut alors s'attendre à un affinement des cibles et à une course à la virtuosité visuelle dans les opérations de *defacement*, bien plus qu'à l'avènement d'un « infoterrorisme » projetant des dommages matériels et physiques par la déstabilisation des « infrastructures nationales critiques » (CNIs) d'un Etat.

Depuis quelques années, la littérature sur la menace « cyberterroriste »[72] n'en est pas moins florissante, agitant le spectre de guerres électroniques imminentes. Ainsi la revue *Terrorism and Political Violence* a-t-elle largement ouvert ses colonnes aux analystes de l'« infoguerre » (*information warfare*). Pour Lorenzo Valeri et Michael Knights, celle-ci peut être définie comme « l'ensemble des activités conduites par certains individus et/ou certains groupes en vue d'atteindre des objectifs stratégiques et politiques spécifiques en portant atteinte à l'intégrité, à l'accessibilité et à la confidentialité des données collectées, stockées et transférées à l'intérieur des systèmes d'information connectées à l'internet » (DEVOST, HOUGHTON, POLLARD, 1997 : 17). Pour ces Cassandres de la guerre électronique, la vulnérabilité des infrastructures nationales critiques et les rancœurs ou la vénalité de certains *hackers* encourageraient les actions « cyberterroristes » et « quand les petits génies de l'informatique rejoindront les groupes terroristes conventionnels, tout porte à croire que leur usage des technologies informatiques se banalisera et que les tactiques relevant du terrorisme de l'information s'intégreront à des répertoires tactiques hybrides » (POST, RUBY, SHAW, 2000 : 117). Certains auteurs appellent pourtant à tempérer ces discours

[71] Le groupe, composé de trois jeunes Brésiliens et de deux Pakistanais, a récemment éclaté, les deux Pakistanais s'étant trouvés exclus du groupe, qui a depuis renoncé à défendre des causes politiques ; cf. http://underground.cz/hacked/www.intem.cz/.

[72] Rappelons que le terme est apparu dans les années 1980 sous la plume de Barry Collin, chercheur à l'Institute for Security and Intelligence de Californie.

alarmistes agitant le spectre d'un « Pearl Harbor électronique »[73]. Ainsi Matthew Devost, Brian Houghton et Neal Allen Pollard suggèrent-ils que « les infrastructures mondiales de l'information offrent aux terroristes de précieuses cibles tactiques et opérationnelles, ouvrant la possibilité de synergies destinées à atteindre des objectifs plus vastes de manière plus efficace et plus médiatique. Mais l'importance du terrorisme de l'information en tant que menace technologique stratégique (…) ne doit pas être exagérée » (DEVOST, HOUGHTON, POLLARD, 1997). Divers éléments relativisent en effet l'hypothèse d'une menace cyberterroriste de grande ampleur : (1) la complexité et la sécurisation des systèmes informatiques critiques ; (2) la préférence des groupes terroristes contemporains pour des méthodes plus classiques et plus visibles : détournements d'avions, prises d'otages, voitures piégées, etc. ; (3) la dépendance croissante de ces groupes vis-à-vis des nouvelles technologies de l'information en matière de communication et de médiatisation ; (4) le nombre limité des sites visés par les *hackers* politisés, agissant généralement par conviction idéologique contre leurs propres autorités nationales ou contre certaines multinationales (POST, RUBY, SHAW, 2000).

Les opérations de cyberterrorisme avéré sont donc encore extrêmement rares. Le cas des « Internet Black Tigers » mentionné plus haut est régulièrement cité comme un exemple d'« infoguerre » au même titre que la diffusion de virus ou les opérations de « déni d'accès » contre des sites de commerce en ligne. Si ces actions sont probablement appelées à se multiplier, elles relèvent d'opérations hacktivistes occasionnant des dommages économiques affectant des usagers privés, plutôt que de véritables attaques cyberterroristes visant à causer la mort et/ou à déstabiliser un gouvernement. Ainsi, à l'heure actuelle, « la voiture piégée demeure en fait une bien plus grande menace que les bombes logiques » (DENNING, 2000) et la guerre électronique n'apparaît pour l'instant envisageable que dans le cadre de conflits inter-étatiques, du fait de l'ampleur des moyens financiers et technologiques qu'elle requiert. Ainsi les discours et les pratiques de cyber-défense ne s'adressent-ils encore qu'à un « tigre en papier ». Il ne s'agit pas pour autant de minimiser leurs enjeux, dans la mesure où la construction sociale de la menace cyberterroriste témoigne de la volonté de « l'Etat cyborg » de dompter la « machine de guerre » électronique qu'a engendré le cyberespace et, par là même, de la retourner « contre les nomades et tous les destructeurs d'Etat » (DELEUZE & GUATTARI, 1981 : 521).

[73] Le mot est de Robert Marsh, ex-chef de la Commission présidentielle américaine chargée de la protection de l'infrastructure nationale critique.

CONCLUSION

On aurait tort de sous-estimer les enjeux des « politiques de l'internet » qui, dans leur variante contestataire ou disciplinaire, auront des conséquences décisives sur l'avenir de nos sociétés. Force est cependant de reconnaître qu'à l'heure actuelle, hacktivistes et cybernationalistes peinent à inventer des répertoires d'action distincts de ceux qui existent hors ligne (la pétition, la grève, le *sit-in*, le vandalisme, etc.) et la plupart d'entre eux insistent sur la complémentarité des mobilisations dans l'espace réel et dans l'espace virtuel. Le recours au *cracking* à des fins politiques est en outre contesté par la plupart des internautes. Ainsi un des interlocuteurs de Fabien Granjon, co-fondateur de Samizdat, lui a-t-il confié : « Alors là, pour avoir organisé ce genre de chose plusieurs fois, je peux te dire que ça passe très mal dans le milieu des internautes. Tu te tailles vite une réputation de khmer activiste ou de terroriste. Non, ça passe très mal » (GRANJON, 2001 : 109). Au final, il semble donc que « l'internet ne change pas tant les personnes qu'il leur permet plutôt de mieux faire ce qu'elles font d'habitude » (DAHLGREN, 2000 : 175). Ce constat est particulièrement évident en ce qui concerne les procès de subjectivation auxquels s'articulent la plupart des conflits contemporains. Comme le montre l'exemple du cybernationalisme, il est encore trop tôt pour parler d'identités numériques. Le virtuel ne saurait opérer comme une matrice de subjectivation autonome : les images de soi et des autres émises et reçues dans le cyberespace dérivent de celles du monde réel et non l'inverse, comme dans les romans de Philip K. Dick et les essais de Howard Rheingold. Les émigrés pendjabis naviguant sur des sites khalistanis ne s'inventent pas une nouvelle identité, pas même un nouvel « état d'esprit », comme le prétend l'un de nos interlocuteurs cité plus haut. Ces sujets politiques s'aident du cyberespace dans leur quête d'eux-mêmes et de leur groupe(s) d'appartenance(s), puisque « le fonctionnement des objets techniques peut être, du point de vue des individus qui y sont engagés, un lieu essentiel de la mise à l'épreuve et de la révélation de l'identité personnelle » (DODIER, 1995 : 221), mais ils y trouvent rarement la source de nouvelles valeurs et affiliations. Il est donc trop tôt pour parler de « sujets politiques numériques », tant le réel continue d'imprimer sa marque sur le virtuel. Comme le souligne Fabien Granjon, « les échanges électroniques ne se substituent […] pas aux contacts physiques, ils les complètent et permettent d'entretenir des liens essentiels dans l'intervalle des rencontres » et, « plus la dimension identitaire est un élément structurant du groupement militant, plus il semble que le besoin de se rencontrer autrement que par le biais du courrier électronique soit envisagé comme une nécessité », d'autres contacts se satisfaisant, par contre, de leur virtualité (GRANJON, 2001 : 83, 97). Les changements les

plus importants que promet la virtualité ne s'opèreront donc probablement pas tant au niveau des sujets politiques que des Etats, la légitimation globale des pratiques de cyber-surveillance, dans le contexte post-11 septembre 2001, indiquant que l'Etat n'a pas dit son dernier mot dans l'espace-monde réticulé qui se constitue sous nos yeux.

Pour certains auteurs, la souveraineté de l'Etat-nation et la pertinence du nationalisme se trouveraient menacées par l'avènement du cyberespace : « le rôle de l'Etat-nation va se trouver bouleversé de manière spectaculaire [dans un avenir proche] et il n'y aura pas plus de place pour le nationalisme que pour la variole » (NEGROPONTE, 1996 : 236). Cette approche radicale s'appuie sur une définition classique de l'Etat, appréhendé à travers « l'espace et le lieu, la géométrie et la géographie », c'est-à-dire « en termes de traces physiques (…), de contours ou de frontières » (EVERARD, 1999 : 7). A y regarder de plus près, force est pourtant de constater la résilience de l'acteur étatique dans l'espace-monde contemporain, même si l'Etat qui s'y redéploie se distingue, par bien des côtés, de son parent westphalien. Jerry Everard suggère alors de « désagréger l'Etat » et de le regarder se redéployer dans le cadre d'un processus de « cyborgisation », c'est-à-dire à travers « l'essor d'une relation symbiotique entre l'Etat et le système global dans lequel il s'emmêle de façon inextricable, dans une toile de structures communicationnelles » (*ibid* : 44). La principale fonction de l'Etat consisterait donc désormais à assurer l'interface « entre les êtres humains et les réseaux qui les connectent » (*ibid* : 80). Ce processus conduirait, pour Everard, du passage de « l'Etat-auteur » foucaldien à un « Etat-rhizome » deleuzien, fonctionnant sur le modèle du « corps sans organe » et travaillé par la déterritorialisation. L'Etat se réinventerait donc actuellement dans le mouvement, dans le « flux à quanta » (le « *soft-power* » (NYE, 1990), la « décharge » aux acteurs privés (HIBOU, 1999)) plutôt qu'à travers l'affermissement des « lignes à segments » (le territoire, la souveraineté) sur lesquelles il s'appuyait jusqu'alors.

Cette résilience de l'Etat peut être envisagée à trois niveaux : (1) dans le nouveau rôle des acteurs étatiques au sein de l'économie mondiale, notamment à travers leur soutien politique ou financier à leur « *e-business* » national ainsi qu'à travers leur aide aux exclus de l'Eden numérique ; (2) dans la tentative de régulation politique de l'internet, *via* l'adoption de textes de lois destinés à lutter contre la « cybercriminalité », au niveau national et international ; (3) dans la construction sociale d'une prétendue menace « cyber-terroriste », légitimant des programmes de « cyberdéfense » se concentrant sur la sécurisation des infrastructures communicationnelles, en partenariat avec certains acteurs non-étatiques (les *hackers* « retournés ») ; parallèlement à cette « guerre de position » électronique, il est également possible que se développent, à l'avenir, de véritables « guerres de manœuvres »

informatiques opposant des Etats usant d'armes « sémantiques » (distribuant de fausses informations à l'adversaire) et surtout « syntactiques » (destinées à endommager ses systèmes informatiques) (EVERARD, 1999 : 106).

Ainsi, assiste-t-on actuellement à l'émergence d'un « Etat-cyborg » dont la principale fonction tient à un rôle d'interface entre citoyens et réseaux d'échange et de discussion mondiaux, adaptant à l'ère électronique les fonctions modernes de l'Etat comme « agent voyer, convertisseur ou échangeur routier » (DELEUZE & GUATTARI, 1981 : 480). Si l'essor de cet « Etat-cyborg » s'inscrit dans la longue durée, il ne se fonde pas moins sur de nouveaux modes de gouvernance, tant en termes de sociologie de ses acteurs (un nombre croissant d'acteurs non-étatiques étant conviés à la gestion des affaires de la collectivité) que d'instruments de l'action publique. Paul Frissen relève ainsi le rôle croissant des technologies de l'information dans les systèmes de gouvernance contemporains : « l'administration publique utilise les technologies de l'information et de la communication à des fins d'organisation interne, pour ses opérations, pour ses transactions, pour la mise au point et l'application des politiques publiques, à des fins de surveillance et de discipline, [ainsi que] pour informer les politiques, les citoyens et les groupes sociétaux. L'administration publique se préoccupe également des technologies de l'information et de la communication en tant qu'objets de régulation et de *policy-making* » (FRISSEN, 1997 : 111). Les modes de gouvernance contemporains peuvent apparaître plus ouverts, plus fluides, que l'exercice du gouvernement caractéristique de la modernité westphalienne. Reste qu'en se projetant dans le cyberespace, l'« Etat-cyborg » peut également renforcer sa capacité de contrôle à travers la banalisation de la cyber-surveillance, précipitant l'avènement d'un véritable « panopticon électronique ». En d'autres termes, la « désagrégation » de l'action publique s'opère souvent en parallèle d'un processus d'invisibilisation des politiques sécuritaires étatiques, qui menace directement les libertés individuelles. Et, bien que les pratiques de cyber-résistance ne constituent pas, à l'heure actuelle, une « menace de défense » (CHOCQUET, 2002), les pratiques de cyber-surveillance ont acquis une légitimité sans précédent dans le contexte post-11 septembre, marqué par l'inquiétant triomphe planétaire des sécuritaires (BIGO, 2002 ; CROWLEY, 2001).

BIBLIOGRAPHIE

Anderson B., *Imagined Communities. Reflections on the Origins and Spread of Nationalism*, Londres, Verso, 1983.

Axel B. K., *The Nation's Tortured Body. Violence, Representation and the Formation of a Sikh Diaspora*, Durham, Duke University Press, 2001.

Bacot J.-P., « Le rôle des magazines illustrés dans la construction du nationalisme au XIXe siècle et au début du XXe siècle », *Réseaux*, 107, 2001, p. 265-293.

Badie B., *La diplomatie des droits de l'homme : entre éthique et volonté de puissance*, Paris, Fayard, 2002.

Balandier G., *Le pouvoir sur scènes*, Paris, Balland, 1992.

Barber B., *Djihad* versus *McWorld. Mondialisation et intégrisme contre la démocratie*, Paris, Desclée de Brouwer, 1996.

Bell D., Kennedy B. M. (eds), *The Cybercultures Reader*, Londres/New York, Routledge, 2000.

Bertrand R., « Quand l'autre est un 'Je'. Dialogues entre la science politique et l'anthropologie sociale », *Raisons politiques*, 4, 2000, p. 7-23.

Bey H., *TAZ. Zone autonome temporaire*, Paris, Editions de l'Eclat, 1997.

Bigo D., « La voie militaire de la 'guerre au terrorisme' et ses enjeux », *Cultures & Conflits*, 44, 2002, p. 5-18.

Blondeau O., « Genèse et subversion du capitalisme informationnel : Linux et les logiciels libres ; vers une nouvelle utopie concrète », *La Pensée*, 317, 1999, p. 21-33.

Breton P., Proulx S., *L'explosion de la communication à l'aube du XXIe siècle*, Paris, La Découverte, 2002.

Burrows R., Featherstone M. (eds), *Cyberspace/Cyberbodies/Cyberpunk: Cultures of Technological Embodiment*, Londres/New Delhi, Sage, 1996.

Capling A., Nossal K. R., « Death of distance or tyranny of distance? The internet, deterritorialization, and the anti-globalization movement in Australia », *The Pacific Review*, 14 (3), 2001, p. 443-465.

Castells M., *La galaxie internet*, Paris, Fayard, 2002.

Cavallaro D., *Cyberpunk and Cyberculture. Science Fiction and the Work of William Gibson*, Londres, Athlone Press, 2000.

Cazenave F., *Les radios libres : des radios pirates aux radios privées*, Paris, PUF, coll. « Que sais-je ? », 1984.

Certeau M. de, *L'invention du quotidien*, tome 1 : *Arts de faire*, Paris, Gallimard, 1990.

Chapman R., « Les radios pirates des années 1960. Radio London et Radio Caroline : analyse comparative », *Réseaux*, 52, mars-avril 1992, p. 59-72.

Chocquet C., « Le terrorisme est-il une menace de défense ? », *Cultures et Conflits*, 44, printemps 2002, pp. 19-64.

Clarke S., « The new localism », *in* S. Clarke, E. Goetz (eds), *The New Localism: Comparative Urban Politics in a Global Era*, Newbury Park, Sage, 1993, p. 1-21.

Cordesman A. H., Cordesman J. G., *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection. Defending the US Homeland*, Westport, Praeger/CSIS, 2002.

Critical Art Ensemble, *The Electronic Disturbance*, Brooklyn, Autonomédias, 1994.

Crowley J., « Triomphe des sécuritaires », *Critique internationale*, 14, janvier 2002, p. 29-33.

Dahlgren P., « L'espace public et l'internet. Structure, espace et communication », *Réseaux*, 100, 2000, p. 159-185.

Davis R., *The Web of Politics: The Internet Impact on the American Political System*, New York, Oxford University Press, 1999.

Deleuze G., *Pourparlers 1972-1990*, Paris, Editions de Minuit, 1990.

Deleuze G., Guattari F., *Capitalisme et schizophrénie*, tome 2 : *Mille plateaux*, Paris, Editions de Minuit, 1981.

Denning D., « Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy », *in* J. Arquila, D. Ronfedt (eds), *Networks and Netwars: the Future of Terror, Crime, Militancy*, Santa Barbara, RAND, 2001, p. 239-288.

Denning D., « Cyberterrorism », Testimony before the special oversight panel on terrorism, Committee on armed services, US House of Representatives, 23 mai 2000 ; disponible à l'adresse suivante : http://www.terrorism.com/documents/denning-testimony.shtml.

Detienne M., Vernant J.-P., *Les ruses de l'intelligence. La mètis des Grecs*, Paris, Flammarion, 1974.

Deutsch K., *Nationalism and Social Communication: An Enquiry into the Foundations of Nationality*, Cambridge/Londres, MIT Press, Chapman and Hall, 1953.

Devost M. G., Houghton B. K., Pollard N. A., « Information terrorism: Political violence in the information age », *Terrorism and Political Violence*, 9 (1), printemps 1997, p. 72-83.

Dibona C. (ed.), *Open Sources: Voices from the Open Source Revolution*, Pékin/Londres, O'Reilly & Associates, 1999.

Dieckhoff A., *La nation dans tous ses Etats*, Paris, Flammarion, 2000.

Dodier N., *Les hommes et les machines : la conscience collective dans les sociétés technicisées*, Paris, Métailié, 1995.

Dodge M., Kitchin R., *Mapping Cyberspace*, Londres, Routledge, 2001.

Douglas S., *Inventing American Broadcasting (1899-1922)*, Baltimore, Johns Hopkins University Press, 1987.

Elkins D. J., « Globalization, telecommunication, and virtual ethnic communities », *International Political Science Review*, 18 (2), 1997, p. 139-152.

Everard J., *Virtual States. The Internet and the Boundaries of the Nation-State*, Londres/New York, Routledge, 1999.

Flichy P., « Internet ou la communauté scientifique idéale », *Réseaux*, 97, 1999, p. 77-120.

Flichy P., « La place de l'imaginaire dans l'action technique », *Réseaux*, 109, 2001, p. 51-73.

Flichy P., « Technologies fin de siècle : l'internet et la radio », *Réseaux*, 100, 2000, p. 249-271.

Flichy P., *L'imaginaire d'internet*, Paris, La Découverte, 2001.

Foucault M., « Afterword: The subject and power », *in* H. L. Dreyfus, P. Rabinow, *Michel Foucault. Beyond Structuralism and Hermeneutics*, Londres, Harverster Wheatsheaf, 1982, p. 208-226.

Frau-Meigs D., « Technologie et pornographie dans l'espace cybernétique », *Réseaux*, 77, 1996, p. 37-60.

Frissen P., « The virtual state. Postmodernisation, informatisation and public administration », *in* B. Loader (ed.), *The Governance of Cyberspace*. *Politics, Technology and Global Restructuring*, Londres/New York, Routledge, 1997, p. 111-125.

Froehling O., « The cyberspace 'war of ink and internet' in Chiapas, Mexico », *The Geographical Review*, 87 (2), 1997, p. 291-307.

Gayer L., « The globalization of identity politics: The Sikh experience », *International Journal of Punjab Studies*, 7 (2), juillet-décembre 2000, p. 223-262.

Gellner E., *Nations and Nationalism*, Oxford, Blackwell, 1983.

Gibson W., *Neuromancer*, Londres, Harper Collins, 1984.

Gibson W., *Count Zero*, Londres, Harper Collins, 1986.

Gibson W., *Mona Lisa Overdrive*, Londres, Harper Collins, 1988.

Giddens A., *Modernity and Self-Identity. Self and Society in the Late Modern Age*, Stanford, Stanford University Press, 1991.

Gramsci A., *Selection from the Prison Notebooks*, Londres, Lawrence and Wishart, 1971.

Granjon F., *L'internet militant. Mouvement social et usage des réseaux télématiques*, Paris, L'Harmattan, 2001.

Guillaume M., « La maîtrise virtuelle de l'espace réel », *Réseaux*, 100, 2000, p.59-79.

Guisnel J., *Guerres dans le cyberespace*. *Services secrets et internet*, Paris, La Découverte, 1995.

Gunawardena S., « Constructing cybernationalism: Sikh solidarity *via* the internet », *International Journal of Punjab Studies*, 7 (2), juillet-décembre 2000, p. 263-322.

Haas P. M., « Introduction: Epistemic communities and international policy coordination », *International Organization*, 46 (1), hiver 1992, p. 1-35.

Hafner K., Markoff J., *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Londres, Fourth Estate, 1991.

Hall S., « The new ethnicities », *in* J. Donald, A. Rattansi (eds), *Race, Culture and Difference*, Londres, Sage, 1992, p. 252-260.

Hibou B. (dir.), *La privatisation des Etats*, Paris, Karthala, 1999.

Hill K., Hugues J., *Cyberpolitics. Citizen Activism in the Age of the Internet*, Lanham, Rowman and Littlefield, 1998.

Hillis K. « A geography of the eye: The technologies of virtual reality », *in* R. Shields (ed.), *Cultures of Internet. Virtual Spaces, Real Histories, Living Bodies*, Londres/New Delhi, Sage, 1996, p. 70-98.

Hiltz S. R., Turroff M., *The Network Nation*. *Human Communication* via *Computer*, Reading, Addison-Wesley, 1978.

Himanen P., *The Hacker Ethic and the Spirit of the Information Age*, New York, Random House, 2001.

Holmes D. (ed.), *Virtual Politics: Identity and Community in Cyberspace*, Londres, Sage, 1997.

Huizinga J., *Homo Ludens. A Study of the Play Element in Culture*, Boston, The Beacon Press, 1950.

Jouet J., « Retour critique sur la sociologie des usages », *Réseaux*, 100, 2000, p. 487-521.

Jouet J., « Pratiques de communication et figures de la médiation. Des médias de masse aux technologies de l'information », *in* P. Beaud (dir.), *Sociologie de la communication*, Issy les Moulineaux, CNET, 1997, p. 291-312.

Jordan T., Taylor P., « A sociology of hackers », *The Sociological Review*, 46 (4), novembre 1998, p. 757-780.

Jordan T., *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Londres, Routledge, 1999.

Keck M., Sikkink K., *Activists Beyond Borders*. *Advocacy Networks in International Politics*, Ithaca, Cornell University Press, 1998.

Keck M., Sikkink K., « Historical precursors to modern transnational social movements », *in* J. Guidry *et al* (eds), *Globalization and Social Movements. Culture, Power and the Transnational Public Sphere*, Ann Arbor, The University of Michigan Press, 2000, p. 35-53.

King A. (ed.), *Global Cities: Post-Internationalism and the Internationalization of London*, Londres, Routledge, 1990.

Lafrance J.-P., « Le point sur… Le laboratoire internet », *Réseaux*, 77, 1996, p. 171-183.

Leary T. F., Entretien avec Richard E. Cytowic, « Sinsory overmode », *Mondo 2000*, 12, 1994, p. 77-86.

Lee E., *The Labour Movement and the Internet: The New Internationalism*, Londres, Pluto Press, 1997.

Levy S., *Hackers: Heroes of the Computer Revolution*, New York, Doubleday, 1984.

Loader B., « The governance of cyberspace », *in* B. Loader (ed.), *The Governance of Cyberspace*. *Politics, Technology and Global Restructuring*, Londres/New York, Routledge, 1997, p. 1-19.

Lyon D., « Cyberspace sociality. Controversies over computer-mediated relationships », *in* ibid, p. 23-37.

Lyon D., *The Electronic Eye. The Rise of Surveillance Society*, Cambridge, Polity Press, 1994.

Mandaville P., « Territoriality and translocality: Discrepant idioms of political identity », *Millenium*, 28 (3), 1999, p. 653-673.

Mandaville P., *Transnational Muslim Politics: Reimagining the Ummah*, New York, Routledge, 2001.

Margolis M., Resnick D., *Politics as Usual: The Cyberspace Revolution*, Thousand Oaks, Sage, 2000.

Marx L., *The Machine in the Garden: Technology and the Pastoral Ideal in America*, New York, Oxford University Press, 1964.

Mattelart A., *Histoire de l'utopie planétaire. De la cité prophétique à la société globale*, Paris, La Découverte, 2000.

Moody G., *Rebel Code: Linux and the Open Source Revolution*, Cambridge, Mass., Perseus Pub., 2001.

Nazeri H., « Imagined cyber communities: Iranians and the internet », *Middle East Studies Association Bulletin*, 30 (2), décembre 1996, p. 158-163.

Negri A., Hardt M., *Empire*, Paris, Exils, 2000.

Negroponte N., *Being Digital*, Londres, Hodder & Stoughton, 1996.

Nye J., *Bound to Lead. The Changing Nature of American Power*, New York, Basic Books, 1990.

Pavlicek R., *Embracing Insanity: Open Source Software Development*, Indianapolis, SAMS, 2000.

Poissenot C., Sadoudi H., « Usages et représentations d'internet », *Documentaliste*, 37 (1), 2000, p. 14-27.

Post J. M., Ruby K. G., Shaw E. D., « From car bombs to logic bombs: The growing threat from information terrorism », *Terrorism and Political Violence*, 12 (2), été 2000, p. 97-122.

Pouligny B., « Acteurs et enjeux d'un processus équivoque. La naissance d'une 'internationale civile' », *Critique internationale*, 13, 2001, p. 163-176.

Quere L., « Espace public et communication. Remarques sur l'hybridation des machines et des valeurs », *in* P. Chambat (dir.), *Communication et lien social*, Paris, Descartes/Cité des sciences et de l'industrie, 1992, p. 29-49.

Raymond E., Young B., *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*, Pékin/Cambridge, O'Reilly & Associates, 1999.

Rheingold H., *The Virtual Community. Homesteading on the Electronic Frontier*, Cambridge, MIT Press, 1993.

Rigaut P., *Au-delà du virtuel : exploration sociologique de la cyberculture*, Paris, L'Harmattan, 2001.

Robertson R., « Glocalization: Time-space and homogeneity-heterogeneity », *in* M. Featherstone (ed.), *Global Modernities*, New Delhi/Londres, Sage, 1995, p. 25-44.

Robins K., « Au-delà de la communauté imaginée ? », *Réseaux*, 107, 2001, p. 21-39.

Rosenau J., *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World*, Cambridge, Cambridge University Press, 1997.

Roy O., « La communauté virtuelle. L'internet et la déterritorialisation de l'islam », *Réseaux*, 99, 2000, p. 219-253.

Sassen S., *The Global City: New York, London, Tokyo,* Princeton, Princeton University Press, 1991.

Soguk N., Whitehall G., « Wandering grounds: Transversality, identity, territoriality, and movement », *Millenium*, 28 (3), 1999, p. 675-698.

Stephenson N., *Snowcrash*, New York, Bantam Books, 1992.

Sterling B., *Schismatrix*, New York, Ace Books, 1989.

Stone A. R., « Virtual systems », *in* J. Crary, S. Kwinter (eds), *Zone 6: Incorporations*, New York, Zone, 1992, p. 609-621.

Taylor P. A., *Hackers. Crime in the Digital Sublime*, Londres, Routledge, 1999.

Thomson J. E., *Mercenaries, Pirates, and Sovereigns. State-Building and Extraterritorial Violence in Early Modern Europe*, Princeton, Princeton University Press, 1994.

Thompson J. B., « Transformation de la visibilité », *Réseaux*, 100, 2000, p. 189-213.

Torvalds L., « Prologue. What makes hackers tick ? a.k.a. Linus's law », *in* P. Himanen, *The Hacker Ethic*, *op cit*, p. xiii-xvii.

Torvalds L., *Just for Fun: The Story of an Accidental Revolutionary,* New York, Harper Business, 2001.

Trautmann F., *Utilisations d'Internet et démocratie interne à ATTAC*, Mémoire de DEA, IEP de Paris, 2000.

Turkle S., *The Second Self: Computers and the Human Mind*, Londres, Granada, 1984.

Veltz P., *Mondialisation, villes et territoires. L'économie d'archipel*, Paris, PUF, 1996.

Verkaail O., *Inside the Citadel. Fun, Violence and Religious Nationalism in Hyderabad*, *Pakistan*, Ph.D, University of Amsterdam, 1999.

Verlulst S., « Diasporic and transnational communication: Technologies, policies and regulation », *Javnost/The Public*, 6 (1), 1999, p. 29-36.

Viard J., « Les nouveaux enjeux du local », *in* P. Perrineau (dir.), *L'engagement politique*, Paris, Presses de Sciences Po, 1994, p. 387-403.

Warkentin C., *Reshaping World Politics. NGOs, the Internet, and Global Civil Society*, Lanham, Rowman & Littlefield Publishers, 2001.