Technologie, défense nationale et sécurité intérieure : un ménage à trois dysfonctionnel[1]

Benoît Dupont
Professeur agrégé
Centre International de Criminologie Comparée, Université de Montréal
benoit.dupont@umontreal.ca
Tel : +1 (514) 343-6111 poste 2586
Fax : +1 (514) 343-2269

Chapitre paru dans La militarisation des appareils policiers, dirigé par Frédéric Lemieux et Benoît Dupont, Les Presses de L'Université Laval, Québec, 2005, pp. 135-156.

[1] Je tiens à remercier F. Lemieux et M. Cusson, dont les suggestions m'ont permis d'améliorer ce chapitre.

Comme le montrent Ericson et Haggerty dans le chapitre précédent, le transfert de technologies du secteur militaire vers le secteur de la sécurité intérieure a connu une nette accélération depuis la fin de la guerre froide, lorsque le complexe industriel de l'armement a dû trouver de nouveaux débouchés pour sa production. Loin d'être considérée comme un développement naturel et anodin par les observateurs, cette tendance est au contraire présentée comme une contamination des valeurs et des pratiques policières par le militaire, entraînant un abaissement préoccupant des critères d'usage de la force et un recours intensif à la surveillance des populations.

Cette appréhension est souvent appuyée de références littéraires renvoyant à l'œuvre de George Orwell, qui a imaginé une société totalitaire dans laquelle le pouvoir politique exerce son emprise sur les citoyens par le biais d'une technologie omnisciente et omnipotente (Orwell 1980). Philip K. Dick a également écrit sur les limites prédictives de la technologie dans le cadre de la lutte contre le crime, assignant à l'usage irraisonné de celle-ci un risque de dépérissement des libertés individuelles (Dick 1956). Ces œuvres de science-fiction sont aujourd'hui ancrées dans l'imaginaire populaire en raison de leur prescience, tout particulièrement en ce qui concerne l'usage intensif de l'information par les forces de l'ordre dans un but de connaissance des phénomènes criminels. Bien entendu, le 1984 d'Orwell dénonçait avant tout la dictature sur les esprits d'une idéologie niant le droit à la différence, le « Big Brother », mais son œuvre est aujourd'hui souvent entendue comme une dénonciation du pouvoir anti-individualiste et déshumanisant des moyens technologiques eux-mêmes.

Cette résistance trouve principalement ses origines dans la théorie de la séparation des fonctions de défense extérieure et de défense intérieure en germe dès l'avènement de l'idée d'État moderne. Le traité de Westphalie, signé par les puissances européennes en 1644, reconnaît pour la première fois des frontières permanentes aux États, qui se dotent d'armées permanentes pour en protéger l'intégrité, ce qui établit une cassure nette avec la pratique des bandes armées de mercenaires, facteur d'insécurité, de violences et d'abus divers. Dans le prolongement direct de cet acte fondateur, le rapprochement technologique contemporain est alors interprété comme annonciateur d'un estompement des différences qui établissaient une partition claire entre police et armée, garante du libre exercice des droits et libertés individuels. Un tel déterminisme technologique, qui assimile l'adoption d'une technologie développée dans un contexte donné à l'adoption des autres caractéristiques institutionnelles propres à ce contexte doit cependant être nuancé. On peut d'abord réfuter cet argument en prenant plus de recul et en considérant les transferts technologiques opérés à l'échelle de la société toute entière : les innovations militaires ayant connu une application et un perfectionnement civil dans le domaine des télécommunications, de la médecine, de l'agriculture ou du transport sont innombrables, et il serait bien entendu exagéré d'affirmer que ces domaines ont été para-militarisés du seul fait de leur accès à des technologies de défense. D'autre part, comme le souligne Jean-Paul Brodeur (2003), ces cauchemars d'une surveillance politique et sociale généralisée sont « trop rationalistes pour se réaliser ». De plus, au niveau bilatéral sécurité intérieure–défense nationale, un examen plus approfondi des arguments avancés fait ressortir la superficialité des théories de la militarisation par la technologie.

La littérature existante assume d'abord que ces transferts s'opèrent dans une seule direction, du militaire vers le policier, ce qui indiquerait de façon indéniable l'emprise du premier sur le second. S'il est vrai que les flux technologiques obéissent à cette logique, on doit cependant souligner que certains efforts en recherche et développement du secteur de la défense

répondent à de nouvelles demandes et logiques d'intervention qui s'inspirent plus du maintien de l'ordre en tant que fonction policière que du conflit traditionnel. Les missions de maintien de la paix font dorénavant partie intégrante des mandats confiés aux forces armées, et celles-ci ont dû adapter leurs outils à cette nouvelle réalité. Le caractère unidirectionnel souligné plus haut doit donc être nuancé.

Ensuite, la rationalité des transferts est essentiellement conçue comme politique, répondant à un effort d'intensification du contrôle social sur les populations, qu'elles soient effectivement ou potentiellement dangereuses. Si cette dimension ne peut être rejetée, elle doit cependant être intégrée dans un assemblage plus complexe de facteurs économiques, organisationnels et culturels qui n'obéissent pas nécessairement à une rationalité aussi homogène et tranchée. Qui plus est, les technologies de sécurité importées du secteur militaire sont associées implicitement à une efficacité qui est loin d'être garantie. De nombreux facteurs viennent en effet en atténuer les effets.

Enfin, le rôle du secteur en pleine expansion de la sécurité privée est négligé, bien qu'il représente un marché bien plus lucratif que celui de la sécurité publique pour les produits issus de la technologie militaire. De même, la résistance sociale aux technologies de contrôle retourne contre les forces de l'ordre les mêmes technologies qui ont fait l'objet d'un transfert en provenance du complexe militaro-industriel. Avant de poursuivre, il est important de préciser que le propos de cet article se limite aux transferts technologiques d'un secteur à l'autre et à leurs implications. L'utilisation d'unités militaires dans des missions de sécurité intérieure du fait de leur capacité à mettre en œuvre des technologies ou des équipements particuliers –la militarisation des fonctions policières– ne sera pas abordée ici, dans la mesure où elle résulte de décisions organisationnelles et politiques ponctuelles, comme ce fut le cas aux États-Unis lors de la guerre initiée par les gouvernements Reagan et Bush contre la drogue ou l'immigration clandestine en provenance du Mexique (Dunn 2001).

Les termes imprécis de l'échange défense-police dans le développement des technologies de sécurité

Une des caractéristiques principales des écrits sur les transferts technologiques entre la défense nationale et la sécurité intérieure est leur relative simplicité conceptuelle : un secteur dominant et s'appuyant sur une industrie puissante, la défense, « coloniserait » un secteur d'activité « fragile », la police. Dans cette perspective, la vulnérabilité de la police serait augmentée par les exigences en matière de respect des droits individuels auquel elle doit se conformer. Les transferts sont ici construits de manière unidirectionnelle et non problématique. Pourtant, les termes de l'échange technologique entre les deux domaines d'activité sont loin d'être aussi simples qu'il n'y paraît. On prendra pour exemple le cas des technologies afférentes aux armes non létales, qui pose la question des critères relatifs à l'usage de la force, et nous projette au cœur du problème des liaisons dangereuses qu'entretiennent la police et l'armée.

Ces armes sont utilisées par les unités spécialisées de la police lors d'assauts violents afin de minimiser le recours aux armes plus conventionnelles, mais elles se répandent également entre les mains des policiers en uniforme, étant alors présentées comme un outil efficace de maîtrise des individus ou des groupes violents rencontrés lors des interactions routinières avec le public. Dans le premier cas, l'usage d'une force disproportionnée destinée à « choquer » ceux contre qui elle est dirigée et à anéantir toute capacité de résistance relève sans nul doute de l'adoption des règles d'engagement militaires, mais se trouve par définition circonscrit à

un nombre réduit de situations extrêmes. Dans le second cas de figure, leur potentiel de banalisation de l'usage de la force, sous le prétexte que celle-ci ne se trouve plus automatiquement associée à des séquelles permanentes, mérite d'être examiné.

Les armes non létales : une technologie contestée

La technologie des armes non-létales constitue un champ particulièrement fertile pour les industriels de la sécurité. Les armes non létales représentent en effet un marché florissant sur lequel opéraient en 1998 plus de 856 sociétés issues de 47 pays (Wright 1998). On inclut dans ce secteur virtuellement impossible à décrire en raison de sa diversité les armes qui émettent des chocs électriques (pistolets, filets, boucliers, etc.), les gaz incapacitants et irritants de toutes natures, et les armes kinésiques comme les balles en caoutchouc et en plastique ou les *flash-balls* (Chambon 2002).

Utilisées initialement par les unités de maintien de l'ordre, les armes non létales figurent dorénavant dans l'équipement de base des policiers en uniforme, sous la forme de gaz divers (lacrymogène, au poivre…) ou de *tasers*, qui génèrent des décharges électriques paralysantes. Leur usage est communément légitimé par l'option additionnelle qu'elles offrent aux policiers dans le continuum de l'usage de la force, avant d'avoir à recourir aux moyens extrêmes. Ces armes permettraient ainsi de stopper la progression ou l'escalade de la violence en incapacitant ceux vers qui elles sont dirigées sans toutefois les blesser de manière durable. Elles représenteraient ainsi un moyen de stabiliser l'intensité de la force déployée lors d'interactions violentes entre la police et certains membres du public.

L'une des objections principales soulevées à cet argument souligne toutefois le caractère contre-intuitif de celui-ci. Des « seuils de retournement » viennent en effet remettre en cause la rationalité technicienne qui l'inspire (Ellul 1988) : la volonté de rationaliser des comportements humains conduit souvent à un point de retournement où explose l'irrationnel, où le résultat atteint n'a plus qu'une étroite parenté avec celui qui était escompté, quand il n'y est pas totalement opposé. L'adoption des balles en caoutchouc par la police d'Irlande du Nord dans les opérations de guérilla urbaine contre les indépendantistes catholiques illustre parfaitement ce phénomène. Officiellement adoptée pour réduire le nombre des victimes parmi la population et aboutir à une désescalade dans l'emploi de la force par les deux camps, cette stratégie produisit l'effet inverse. Les blessures extrêmement graves infligées par ces armes, que l'usage à bout portant rendit aussi dangereuses que des armes conventionnelles, ne firent que renforcer la détermination des manifestants qui redoublèrent de violence. Plutôt que de mettre un terme à cette expérimentation visiblement mal conçue, les forces de l'ordre obtinrent alors en dotation des munitions en plastiques, nourrissant le cycle interminable violence-répression.

Ce n'est en effet pas l'intensité de la force déployée lors de l'utilisation des armes non létales qui s'est avérée déterminante, comme le croyaient les promoteurs de cette technologie, mais la fréquence de son usage. Celle-ci ayant augmenté proportionnellement à la diminution du risque de blessures infligées (du moins théoriquement), les bénéfices escomptés ne se sont pas manifestés et ont au contraire été supplantés par une intensification des affrontements. Bien entendu, il est nécessaire de prendre en considération le contexte particulier des accrochages récurrents qui caractérisent le conflit irlandais et qui trouvent leurs racines dans une lutte politique pour l'indépendance d'une région. On retrouve dans une certaine mesure cette configuration dans les zones où les fonctions policières sont remplies dans un arrière-plan de guérilla urbaine, où les protagonistes se connaissent bien –Pays Basque, Palestine, grands

sommets internationaux–, et où la complexité des problèmes est irréductible à l'introduction d'un nouveau « gadget » technologique. Ces situations restent cependant des cas isolés à l'échelle des sociétés occidentales : la grande majorité des incidents impliquant l'usage des armes non létales par la police concernent en effet des événements routiniers lors desquels des suspects opposent une résistance à leur arrestation ou à leur détention. Dans ce contexte, l'interaction entre les parties en présence détermine presque exclusivement l'issue de la rencontre et l'emploi des armes non létales est perçu dans les services de police comme une alternative préférable à l'usage d'une force extrême aux effets irréversibles ou le recours à des techniques de contrôle *ad hoc*. En l'absence de statistiques fiables sur l'usage de ces armes par les services de police[2], il est de toute évidence difficile de généraliser l'argument selon lequel les technologies non létales génèrent des effets contre-intuitifs systématiques, comme il est hasardeux de voir en elles la panacée dans les cas de confrontations violentes.

C'est néanmoins dans cette perspective que doit être interprété l'enthousiasme des organisations policières nord-américaines pour ces nouvelles armes. Depuis le début des années 1990, les services de police ont été confrontés à une inflation de plaintes émanant de citoyens abusivement malmenés et à des jugements accordant à ces derniers des dommages financiers de plus en plus conséquents. Ainsi, la ville de New York versa plus de 70 millions de dollars de dommages et intérêts entre 1994 et 1996 aux victimes d'abus policiers, alors que sur la côte Pacifique, les victimes de la police de Los Angeles obtinrent 80 millions entre 1991 et 1996 (Human Rights Watch 1998). De plus, à l'occasion des événements fortement médiatisés tels que les émeutes déclenchées par l'acquittement des policiers de Los Angeles accusés d'avoir brutalisé Rodney King en 1992[3], ou le désastre du siège contre la secte des Branch Davidians à Waco en 1993, un débat fut lancé sur le manque d'options relatives à l'usage de la force et la propension à une violence mal maîtrisée parmi les divers services de police. Ce débat reprit un certain nombre d'arguments avancés dans un arrêt de la Cour Suprême de 1985[4] qui enjoignait les services de police américains de formuler des politiques plus restrictives d'usage de la force que celles alors en vigueur. Cette « mauvaise presse » conduisit à la signature en 1994 d'un accord de coopération entre la Ministre fédérale de la justice Janet Reno et le Secrétaire adjoint à la défense John Deutch, permettant au Pentagone de transférer certaines technologies non létales aux agences chargées de la sécurité intérieure (Nollinger 1995, Department of Defense et Department of Justice 1994). Cet accord n'est pas exceptionnel, puisque le Ministère de la Justice a également signé des ententes similaires avec le Département de l'Énergie, qui dispose de laboratoires de recherche spécialisés, ou des entreprises travaillant sous contrat pour la NASA (Seaskate Inc 1998). La motivation principale n'était donc pas ici de militariser ou de durcir la réponse policière, mais au contraire de réduire les possibilités de blessures des suspects et le nombre des poursuites légales, tout en maintenant la capacité d'intervention des policiers.

Cette préoccupation, en soi louable, est néanmoins confrontée aux nombreuses questions qui restent en suspends quant à la véritable innocuité de ces armes. Les rares études médicales menées sur ce sujet laissent entendre que ces dernières sont beaucoup moins bénignes que ne

[2] Les rapports annuels des services de police contiennent bien des chiffres sur le nombre d'utilisations justifiées et injustifiées, mais ils nous en apprennent peu sur le profil des incidents et des personnes contre qui il a été fait usage des gaz. Le rapport annuel du Service de Police de la Ville de Montréal signale par exemple laconiquement le décès de deux citoyens suite à l'usage du capsicum (gaz au poivre) en 2000, sans donner plus de détails (SPCUM 2001).

[3] Le bilan final officiel de ces émeutes fut de 60 morts, 2000 blessés et environ 10000 commerces et entreprises détruits (Seaskate 1998 : 40).

[4] Tennessee v. Garner 471 US 1 (1985).

le laissent croire leurs fabricants. Le rapport de la fondation Oméga, réalisé pour le compte de l'Union Européenne (Wright 1998), ou certaines études menées dans les laboratoires militaires sur les armes kinésiques ou les composés chimiques utilisés rappellent que le contexte d'utilisation peut transformer une arme non létale en arme mortelle sans aucune modification technique, ce qui explique que la terminologie employée fasse de plus en plus fréquemment référence à des armes *moins* létales. Les campagnes d'Amnesty International sur l'emploi de ces armes à des fins de torture par les dictatures du monde entier ne font que renforcer cet argument (2001). De plus, les impacts environnementaux et sanitaires à plus long terme de l'emploi de ces armes restent méconnus. Ainsi, certaines armes chimiques telles que les mousses « visqueuses » immobilisantes contiennent des composants cancérigènes (par exemple le Butadiene) ou tombant sous le coup du protocole de Montréal sur la protection de la couche d'ozone (Freon-12 et Dichlorodifluoromethane) (Sautenet 2000).

Technologie unique, besoins multiples

On voit donc qu'en dépit des risques réels associés à l'usage des armes non létales par les services de police, les causes de leur adoption par ces derniers peuvent difficilement être réduites à une volonté de militarisation rampante. On pourrait au contraire faire la proposition inverse : les services de police ont adopté cette technologie pour le potentiel de réduction du recours à la force qu'elle laisse entrevoir, même si les résultats sont loin d'être aussi prometteurs qu'escompté. De même, du côté militaire, les forces armées américaines ont essentiellement axé leurs efforts de développement des armes non létales sur des activités plus proches du maintien de l'ordre et de la gestion de crise que des combats sur le champ de bataille. Ainsi, 70% des ressources budgétaires allouées en 1996 au programme de recherche sur les armes non létales étaient orientées vers des missions de maintien de la paix et des opérations humanitaires (Siniscalchi 1998). Cette technologie traduit en effet un profond changement de paradigme de la doctrine d'emploi des forces armées. Inversant une tendance historique qui avait vu jusque-là une escalade dans la puissance destructrice des armements, pour culminer avec les armes atomiques, bactériologiques et chimiques, les armes non létales marquent la volonté des stratèges militaires de limiter le nombre de victimes et de dégâts matériels dans les conflits modernes (Siniscalchi 1998). Cette soudaine préoccupation, loin de naître d'un sentiment altruiste et pacifique trouve ses origines historiques dans l'adoption par l'armée américaine au cours des années 1990 d'un cadre stratégique reposant sur le constat de la réticence de l'opinion publique à voir les forces américaines engagées dans des conflits longs et coûteux à l'étranger, sur une préférence accordée aux conflits de moins grande intensité, et sur le constat de l'émergence d'acteurs non-étatiques sur la scène internationale, caractérisés par leur très forte intégration aux populations civiles.

L'intervention américaine en Somalie et les violents combats de rues qui la caractérisa, combiné à une réflexion de plus en plus poussée sur le cadre tactique d'utilisation de ce nouveau type d'armement, conduisirent alors le Pentagone à lancer un vaste programme de recherches associant les différents corps de l'armée américaine au sein du Programme Conjoint sur les Armes Non-Léthales[5]. La généalogie de ce programme confié au corps des Marines remonte au début des années 1970, lorsque des futurologues de l'armée américaine (Coates 1970) envisagèrent pour la première fois l'utilisation de technologies non-destructrices. Dès 1993, la première Conférence de Défense Non Létale se tient à l'Université Johns Hopkins, sous le patronage du Laboratoire National de Los Alamos, où fut développée

[5] http://www.jnlwd.usmc.mil/.

la bombe atomique. Cette conférence rassembla plus de 300 participants issus des laboratoires militaires, mais également de l'industrie de l'armement et du monde universitaire.

Si dans la littérature militaire, les armes non-léthales sont présentées avant tout comme un outil de plus à l'arsenal déjà passablement garni des soldats américains, on mentionnera également les travaux de sociologues de l'armée qui insistent sur les changements profonds amenés par la participation croissante aux missions internationales de maintien de la paix. Dès le début des années 1970, Charles Moskos note dans ses observations de contingents canadien, danois, britannique, irlandais, suédois et autrichien opérant à Chypre sous mandat des Nations Unies le développement d'une éthique policière (*constabulary ethic*) parmi les troupes (Moskos 1975). Celle-ci, définie notamment dans les travaux de Morris Janowitz (1960) se caractérise de manière générale par un recours à l'usage de la force restreint aux situations d'auto-défense. Sur le plan opérationnel, l'éthique policière se traduit par une conviction de la part des soldats que des compétences supplémentaires aux aptitudes purement militaires sont requises dans le cadre des missions de maintien de la paix, et que l'efficacité opérationnelle lors ces missions n'est en aucune façon associée à l'usage de la force. Les observations de Moskos, étayées par des indicateurs statistiques, font apparaître qu'une minorité des officiers se reconnaissent dans l'éthique policière au début de la mission (32% le premier mois), mais que la progression de celle-ci est régulière dans le temps pour atteindre 60% à la fin de la mission. Une telle éthique professionnelle, qui vient contrarier un certain nombre de valeurs militaires essentielles comme la force écrasante est désormais profondément ancrée dans les registres d'action des contingents opérant sous mandat de l'ONU. Cette transformation, qui va dans le sens d'une convergence avec le policier est d'ailleurs critiquée par quelques auteurs, qui y voient là une dénaturation de l'efficacité militaire (Dunlap 2001).

Cet exemple, qui ne constitue qu'un fragment des transferts technologiques entre défense nationale et sécurité intérieure nous semble toutefois représentatif d'une complexité plus grande dans les termes de l'échange que la limpidité trompeuse des tenants d'une militarisation liberticide. L'arrêt de la Cour Européenne des Droits de l'Homme, qui a condamné la Turquie dans l'affaire Güleç[6] pour n'avoir pas doté ses forces de police de telles armes lors des manifestations violentes est à cet égard exemplaire. Cette condamnation, faite au nom des principes de justice et de respect des droits de l'homme, qui prescrit quasiment l'usage d'armes non létales nous amène plutôt à proposer une lecture théorique des transferts technologiques qui met l'accent sur l'existence de rationalités concurrentes, certaines facilitant les transferts technologiques entre la défense et la police, d'autres au contraire s'opposant ou encadrant strictement ces transferts.

Les rationalités concurrentes : économie, droit, politique et pratiques opérationnelles

Les raisons des transferts qui peuvent s'opérer entre les laboratoires militaires et les agences policières dépendent en effet beaucoup plus de rationalités concurrentes et parfois même contradictoires que d'une volonté monolithique d'annexion du champ de la sécurité intérieure par celui de la défense nationale. On distinguera ainsi la rationalité économique, la rationalité juridique, la rationalité politique et la rationalité opérationnelle, dont les effets sur l'adoption et l'emploi de nouvelles technologies sont loin d'être uniformes. Ces rationalités ne s'articulent pas entre elles de manière logique, en raison de leur élaboration laborieuse,

[6] Requête no 21593/93 §71.

déterminée principalement par les problèmes ponctuels et contextuels auxquels doivent faire face les agents. Attribuer une signification unique à l'adoption de certaines technologies militaires par certains services de police dans certaines situations revient ainsi à nier cette dimension hautement instable et fragmentée que représente la réalité des praticiens.

Rationalité économique

Si l'on prend comme point de départ la rationalité économique, on a par exemple montré dans une section précédente comment les coûts financiers induits par les dommages et intérêts versés par les services de police américains aux victimes de comportements abusifs ont ouvert un marché pour les armes non-léthales, qui étaient auparavant l'apanage de l'armée. De la même façon, l'une des raisons principales à la forte présence de l'industrie de défense dans le secteur de la sécurité intérieure tient à la taille réduite de ce dernier, et tout particulièrement aux États-Unis, où l'on compte environ 17 000 petits services, 90% d'entre eux disposant de moins de 24 policiers. Cette fragmentation du marché potentiel rend tout effort de promotion extrêmement coûteux pour les entreprises offrant des solutions technologiques aux services de police. De plus, la plupart des services fonctionnent avec des budgets réduits dont l'essentiel est consacré aux salaires de leurs employés (Seaskate Inc 1998). Dans ce contexte, l'expertise nécessaire à la prise de décision lors de l'acquisition de nouvelles technologies est absente et les ressources disponibles pour la recherche et le développement sont minimales, ce qui résulte en une incompatibilité des systèmes et une fragmentation additionnelle. Peter Manning relève ainsi dans le cadre de deux études ethnographiques conduites lors des Jeux Olympiques de Salt Lake City et dans le Massachusetts l'impossibilité pour des agences impliquées de communiquer entre elles autrement que par les lignes téléphoniques classiques, malgré l'équipement radio sophistiqué de chacune d'entre elles (Manning 2003).

Les ressources quasi-illimitées attribuées à l'industrie de défense par le gouvernement américain contrastent alors avec la modestie des budgets policiers : les données disponibles les plus récentes font ainsi apparaître que plus de 53 milliards de dollars ont été accordés dans le budget des États-Unis en 2003 pour les dépenses de recherche et de développement dans le secteur militaire (Department of Defense 2002). Devant un tel déséquilibre, le souhait des autorités policières d'accéder à certaines technologies militaires semble bien en partie guidé par des contraintes économiques. De plus, on peut aussi imaginer pour les mêmes raisons que seules les technologies dont les bénéfices attendus outrepassent les coûts sont considérées, que ce calcul se matérialise ensuite dans les faits ou non. En effet, dans le contexte de frugalité fiscale qui caractérise bon nombre d'organisations policières, l'offre technologique dépasse de loin la demande, voire les besoins. On peut donc sans conteste opposer la rationalité économique contingente à une pure rationalité technique d'efficacité, reposant sur des transferts massifs de la défense nationale vers la sécurité intérieure.

Rationalité juridique

Bien entendu, la rationalité juridique, telle que définie par les décisions judiciaires lors du recours à de nouvelles technologies est également déterminante. Les nombreuses dispositions normatives qui régissent la procédure pénale s'appliquent en effet aux innovations techniques mises en œuvre par la police, contraintes auxquelles les organisations militaires ne sont que rarement exposées. Dans deux arrêts prononcés par les plus hautes instances judiciaires américaines et canadiennes[7], l'emploi par les services de police de caméras à imagerie

[7] Kyllo v. United States (99-8508) 533 U.S. 27 (2001) et R. v. Tessling ONCA C36111 (20030127).

thermique avant (FLIR), capables de détecter des sources de chaleur anormales à travers les murs du domicile a conduit à l'invalidation des procédures intentées. Dans le cas américain comme dans le cas canadien, les arguments avancés par les représentants de forces de l'ordre faisaient état du caractère anodin de cette technologie, qui capte la chaleur émanant des surfaces extérieures d'un bâtiment. Ces « profils de structure » ne seraient pas susceptibles révéler de détails intimes, et ne constitueraient donc pas une perquisition au sens de la loi. Pourtant, les tribunaux ont invalidé cette interprétation, sur la base d'une atteinte intolérable au droit à la vie privée applicable à la résidence. Le Quatrième Amendement de la constitution américaine[8] et l'article 8 de la Charte[9] stipulent en effet que les citoyens ont le droit d'être protégés contre les fouilles, les saisies ou les perquisitions abusives, c'est-à-dire sans mandat judiciaire, et tout particulièrement à leur domicile. Dans les deux arrêts cités, les juges ont estimé que ce droit n'avait pas été respecté, et que toute technologie portant atteinte à l'intégrité du domicile en révélant les activités de ceux qui s'y trouvent, quelles qu'en soit la nature, ne pouvait être utilisée par la police sans mandat. Qui plus est, dans le cas américain, cette interdiction est renforcée par le fait que la police avait utilisé une technologie qui n'est pas d'usage courant et qui est réservée aux interventions militaires et policières, ce qui renforçait son caractère intrusif. La portée de ces arrêts est encore difficile à évaluer, mais certains y voient d'ores et déjà une limite posée à l'usage des technologies de surveillance, notamment dans la sphère privée, même si les conséquences des nouvelles lois anti-terroristes votées en urgence depuis le 11 septembre 2001[10] semblent suspendre certains des droits élémentaires consentis par les gouvernements aux citoyens.

L'espace public est par contraste presque entièrement quadrillé par des technologies de surveillance variées. Les caméras de télévision en circuit fermé font désormais partie intégrante de notre environnement quotidien, et la biométrie semble vouée à un succès similaire, en dépit leurs résultats mitigés (Leman-Langlois 2002, Stanley et Steinhardt 2002). Pourtant, là encore, la rationalité légale influe sur le déploiement des technologies de sécurité, comme en atteste en France la législation sur la vidéosurveillance, qui prescrit la destruction des enregistrements dans un délai ne pouvant pas dépasser un mois[11], à moins qu'ils soient utilisés dans le cadre d'une enquête policière. La réticence des responsables de la sécurité aéroportuaire à mettre en service une nouvelle génération de détecteurs à rayons X à basse intensité (*backscatter*), qui scanne l'anatomie des personnes qui y sont exposées pour détecter la présence d'armes ou d'explosifs relève également de cette incertitude créée par le corpus juridique de protection de la vie privée (Pinsker 2003). Si encore une fois, l'influence de la rationalité juridique repose sur une application inégale des textes qui reste insatisfaisante pour les défenseurs des libertés civiles, les utilisateurs policiers n'en doivent pas moins composer avec elle, et l'intégration de technologies d'inspiration militaire ne se fait pas avec la fluidité absolue qu'on leur prête parfois.

Rationalité politique

Il arrive même que la rationalité politique précède la rationalité juridique dans son rôle de régulation des initiatives policières. On a vu par exemple au lendemain des événements du 11

[8] « Le droit des citoyens d'être garantis dans leur personne, leur domicile, leurs papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou déclaration, ni sans que le mandat décrive particulièrement le lieu à perquisitionner et les personnes ou les choses à saisir ».

[9] « Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ».

[10] USA PATRIOT Act aux États-Unis et Loi C-36 au Canada.

[11] Pour les opérateurs privés, le délai est abaissé à 3 jours. Art 10-4 de la loi No 95-73 du 21 janvier 1995.

septembre se dessiner, aux USA mais également dans les autres pays visés par Al Qaeda, de nouveaux mécanismes de contrôle social basés sur une étroite collaboration entre l'industrie de défense et les agences gouvernementales de sécurité. La création du programme de *Total Information Awareness* (Vigilance Information Totale), rapidement rebaptisé *Terrorist Information Awareness* (Vigilance Information Terroriste) sous la pression de l'opinion publique a ainsi résulté de cette logique. Ce programme technologique tous azimuts a été placé sous la direction de l'Amiral John Poindexter, plus connu pour son implication dans l'Irangate, avant de s'être reconverti temporairement dans le secteur privé. L'objectif du TIA, dans le prolongement de la branche du Pentagone chargé d'encourager la recherche militaire (la DARPA), était d'intégrer les technologies de croisement de l'information afin d'exploiter les masses de données stockées dans les fichiers des administrations et des entreprises américaines. Ce programme devait permettre un traitement des profils virtuels des citoyens (plus tard des terroristes potentiels seulement) afin d'identifier les individus à risque, dans une perspective de lutte contre le terrorisme (Brodeur et Leman-Langlois). Parmi les nouveaux outils en développement, une initiative (le *Policy Analysis Market*) visant à se servir de la capacité des marchés à prédire la probabilité d'événements tels que des attaques terroristes ou des assassinats de dirigeants politiques attira l'attention de plusieurs sénateurs.

Ces derniers furent choqués par la possibilité que le marché virtuel ainsi créé puisse conduire à l'enrichissement de personnes misant sur la déstabilisation de pays ou les succès de groupes terroristes. Quelques jours avant que ce programme ne soit inauguré, le Sénat américain supprima son budget et dissout l'unité qui en était responsable, l'*Information Awareness Office*, l'Amiral Poindexter ayant été poussé à la démission quelques semaines plus tôt (Hulse 2003)[12]. De l'autre côté de l'Atlantique, le Parlement Européen se pose également en garant des libertés individuelles contre les initiatives d'Europol et des services de police, notamment sur le sujet de la rétention des données et de leur transfert vers les agences américaines de police et de renseignement (voir à cet égard l'imposante littérature disponible sur le site Internet de l'Observatoire des Libertés Statewatch[13]). Ces exemples démontrent les transactions et les négociations qui s'opèrent en permanence entre rationalité politique et rationalité technologique, la première n'hésitant pas à remettre la seconde en question la seconde lorsque l'un de ses intérêts essentiels – ici son image de garante du bon fonctionnement de l'exécutif – est en jeu. Il faut donc réitérer notre constat du manque de cohérence des transferts technologiques entre les secteurs militaire et policier, cette relation étant plutôt définie par des avancées, des ruptures et des retours en arrière qui viennent invalider toute idée d'inéluctabilité. Dans cette veine, les prophéties catastrophistes sur l'avènement d'une société de surveillance maximale peuvent être comparées aux pronostics exagérés du Club de Rome sur l'état de la planète au début des années 1970.

Rationalité opérationnelle

Finalement, la rationalité opérationnelle, celle des utilisateurs policiers de ces technologies d'inspiration militaire, dépasse la simple mise en œuvre « mécanique ». Les menaces que font peser l'intégration des technologies militaires et du travail policier sur les libertés individuelles, si elles sont bien réelles, monopolisent l'attention et sous-estiment les facteurs

[12] Il faut cependant signaler l'existence d'autres programmes de recherche menés par la communauté du renseignement, reposant sur des logiques identiques de traitement massif des données : parmi ceux-ci, on signalera le CAPPS 2 (*Computer Assisted Pre-Screening System*), orienté vers le profilage des passagers aériens, et le NIMD (*Novel Intelligence for Massive Data*), piloté par l'organe de recherche de la *National Security Agency*.

[13] www.statewatch.org.

liés à leur emploi, qui en limitent la portée. Les contradictions internes de la technique et leurs effets perturbateurs sont rarement abordés, sous le prétexte que les nouvelles techniques sont adoptées pour des objectifs manifestes, alors que des logiques latentes sont aussi à l'œuvre. Tout autant qu'une efficacité infaillible dans la gestion des risques criminels, c'est la puissance symbolique de la technologie militaire qui est invoquée par les décideurs policiers, à la recherche d'une image de professionnalisme et de modernité. Ceci explique qu'un système technique soit parfois moins valorisé pour sa fonction opérationnelle que pour la fonction symbolique qu'il remplit. Manning a ainsi montré comment les outils d'analyse et de cartographie criminelle, calqués sur les systèmes d'information géographique de l'armée restent sans effets opérationnels notables malgré les progrès des connaissances sur les phénomènes de localisation et de déplacement de la délinquance, et ce en raison de contraintes historiques et organisationnelles (Manning 2001). De plus, si un contrôle accru par la mise en œuvre de nouvelles technologies est effectivement l'un des objectifs manifestes recherché par les décideurs policiers, celui-ci porte autant sur les employés de l'organisation que sur les populations jugées « à risques ». Les syndicats policiers ne s'y trompent pas, qui s'opposent parfois avec virulence à certaines innovations, lorsque le potentiel de ces dernières d'érosion du pouvoir discrétionnaire de leurs membres devient trop intense. Les opérateurs eux-mêmes ne se privent pas d'ajuster les technologies qu'on leur confie à leurs propres besoins. Comme toutes les autres dimensions organisationnelles, la technologie donne lieu à l'éclosion de comportements de jeu qui visent à maximiser les ressources stratégiques de chacun des acteurs. Les individus identifient et exploitent les faiblesses des systèmes mis à leur disposition afin de se réapproprier une autonomie qu'on cherche à leur arracher par le biais de technologies de contrôle qui y sont enchâssées. Tous ces objectifs latents, instables et contradictoires sapent de manière peu spectaculaire mais néanmoins irrésistible l'efficacité des transferts de technologies de sécurité. Ces facteurs exogènes, dépendant des intérêts organisationnels sont de surcroît accentués par des facteurs endogènes qui alimentent les discours et les pratiques de résistance des utilisateurs sur le terrain.

Les technologies transférées, issues de la recherche la plus avancée, sont d'autant plus fragiles qu'elles sont complexes, ce qui entraîne la multiplication des « parasites » et l'ouverture de brèches lors de leur mise en service opérationnelle. Le sophisme du système parfait (Marx et Corbett 1991) montre ses limites, dans notre vie quotidienne comme dans les cycles d'utilisation des technologies policières. Dans les zones urbaines, les ondes radio des systèmes de communication de la police se réverbèrent sur les façades des immeubles, créant des « trous noirs » qui empêchent toute communication. Il en va de même des logiciels sophistiqués et des bases de données relationnelles, dont le fonctionnement est loin d'être aussi dénué de pannes et d'interruptions de service que ne le laissent croire les représentations idylliques des médias et de leurs constructeurs (Leman-Langlois 2002). Le cycle de plus en plus court des innovations techniques signifie qu'une technologie en remplace une autre bien trop rapidement pour que les problèmes de compatibilité puissent être résolus de manière satisfaisante, et que la migration d'un système à un autre se fasse sans accrocs. Ce constat s'applique avec une même fatalité dans les autres domaines économiques, ce qui doit alors nous amener à reconnaître le caractère illusoire de toute tentative de constituer un filet de surveillance aux mailles si serrées qu'il permette de capturer toutes les informations nécessaires au contrôle social d'une société de sécurité maximale. Bien plus que le spectre d'une société où la surveillance de tous par les machines se ferait aux détriments des libertés individuelles et du droit à la vie privée, ce sont plutôt les erreurs découlant des approximations et des failles ouvertes par les conflits de rationalités qui constituent un véritable danger pour la justice et la sécurité des citoyens. On assiste ainsi sans nul doute à des efforts soutenus destinés à interconnecter des moyens technologiques de contrôle social

en perpétuel perfectionnement, mais ces efforts sont simultanément exposés à de nombreuses contestations provenant de rationalités dont nul ne peut présager des conséquences. D'autant plus que les transferts technologiques de la défense nationale à la sécurité intérieure ne peuvent être décrits comme une transaction fermée entre deux groupes d'acteurs clairement identifiés.

Diffusion, dispersion et résistance aux technologies de sécurité

Les technologies de sécurité adaptées de la recherche militaire obéissent en effet beaucoup plus à une logique de diffusion, voire de dispersion, que de simple transfert ou de ruissellement canalisé. Dans la perspective de rationalités concurrentes décrite plus haut, cet éclatement n'est pas sans conséquences, dans la mesure où il accroît les sources de friction entre ces diverses rationalités. La diffusion en dehors des enceintes purement militaires ou policières résulte de l'implication des entreprises privées dans les processus de production de ces technologies, et de leur souci afférent de rentabiliser leurs investissements en mettant leurs produits à la disposition du nombre maximal d'acheteurs, le secteur privé représentant un marché privilégié. De plus, les règles du marché, qui sous-tendent cette « industrie », génèrent une demande pour des technologies de contre-mesure qui est assouvie par des canaux légitimes, mais aussi par des moyens illicites. Enfin, l'ouverture des sociétés modernes, rendue justement possible par les nouvelles technologies issues de la guerre froide[14], permet à des groupes organisés de mettre en œuvre de stratégies de résistance qui s'appuient sur les technologies militaires ayant « ruisselé » de manière incontrôlée vers la société civile.

L'offre et la demande : la mainmise du secteur privé

Contrairement au sens commun, qui imagine une recherche publique menée dans quelques laboratoires gouvernementaux ultrasecrets, les centres de recherche américains qui oeuvrent dans le secteur de la sécurité sont gérés par le secteur privé, sous contrat avec les divers ministères concernés. Le Department of Energy, qui est responsable du développement de technologies afférentes au secteur atomique, mais qui travaille aussi pour le ministère de la défense et le *Department of Homeland Security* a ainsi confié les rênes du laboratoire de Los Alamos à l'Université de Californie[15], alors que les laboratoires nationaux Sandia opèrent sous le contrôle de la multinationale aéronautique Lokheed Martin[16]. De son côté, la DARPA alloue aux entreprises du secteur privé une part importante des fonds que le Pentagone consacre à la recherche. La CIA elle-même a partiellement privatisé son effort de recherche et développement, créant une société de capital-risque chargée d'investir dans les entreprises privées mettant au point des innovations technologiques prometteuses dans le domaine du renseignement – les fameuses *start-ups* qui voient le jour dans les chambres d'étudiants ou dans les garages de leurs fondateurs. Cette société, In-Q-Tel[17], affirmait en novembre 2003 avoir examiné plus de 3 400 propositions et investi dans 40 entreprises. L'industrie qui gravite autour de la recherche militaire est si florissante qu'elle a engendré l'équivalent de la *Silicon*

[14] L'histoire de la naissance du réseau des réseaux, l'Internet, dont les premiers terminaux furent financés par le programme de recherche du Pentagone fait maintenant partie du « mythe » de la révolution informationnelle qui se déroule sous nos yeux depuis une vingtaine d'années (Abbate 1999, Castells 2001). La légende veut que ce nouveau moyen de communication ait été conçu avant tout pour survivre à un conflit atomique entre les USA et l'URSS, qui aurait rayé de la carte de nombreux centres urbains américains.

[15] www.lanl.gov.

[16] www.sandia.gov.

[17] www.in-q-tel.com.

valley californienne dans les environs de Washington. La « vallée des espions » (*Spook valley*) ne compterait ainsi pas moins de 2000 sociétés privées en compétition sur le juteux marché des technologies de sécurité (Murphy 2001)[18]. Les agences gouvernementales constituent le principal client de ces entreprises, mais devant une telle compétition, les clients privés sont également démarchés activement. Les mêmes logiciels de surveillance développés pour les services de renseignement et les organisations policières sont vendus aux cabinets d'audits, aux entreprises de télécommunication, aux banques et aux sociétés de consultants internationales qui s'en servent pour détecter la fraude ou pratiquer le renseignement économique. A cet égard, si la technostructure militaire trouve des débouchés parmi les organisations policières, c'est avant tout le secteur privé qui constitue le marché le plus profitable pour la commercialisation des technologies de sécurité. Jean-Paul Brodeur et Gary T. Marx ont déjà montré dans quelle mesure le développement exponentiel de la sécurité privée reposait sur un recours intensif à la technologie, qu'il s'agisse des caméras de surveillance en circuit fermé, des appareils d'écoute électronique ou des logiciels de croisement des données (Brodeur 2003, Marx 2001), et l'on renverra le lecteur aux références citées pour plus de détails.

Cette très forte intégration des entreprises privées aux processus de conception et de diffusion des technologies de sécurité se fait paradoxalement sur un mode fragmentaire et dispersé qui est bien éloigné d'un *Big Brother* étatique. On voit plutôt se développer une constellation[19] de *Mini Brothers* non gouvernementaux qui représentent un risque égal, si ce n'est supérieur, à celui de leur aîné orwellien, en raison notamment de leur encadrement régulatoire inexistant. La logique du marché qui caractérise ce pan de la sécurité est porteuse de profondes iniquités (Loader 1999, Newburn 2001), le plus souvent au détriment des plus pauvres, et dans cette perspective, se focaliser exclusivement sur les dangers que fait peser la surveillance de l'appareil d'État sur les citoyens est trop réducteur[20]. Les outils de surveillance, qu'ils soient mis en œuvre par le gouvernement ou des intérêts privés sont en effet inutiles s'ils ne trouvent pas des données à mettre en relation afin de pouvoir étendre leurs capacités prédictives, et ce sont les entreprises privées qui encore une fois, se chargent d'acquérir et de structurer des données éparses pour constituer, dans des conditions à la limite de la légalité, des banques de profils virtuels offertes au plus offrant. Ces entreprises de « consolidation des données », comme elles aiment à se faire connaître, offriront peut-être un jour un service qui permettra à ceux qui sont prêts à payer de « disparaître » de leurs fichiers.

L'impossible contrôle des technologies de contrôle

Car la marchandisation de la sécurité incite également au développement d'un marché de la contre-mesure, où se côtoient des opérateurs plus ou moins légitimes, qui offrent toute une palette de produits et de services eux-mêmes issus de la recherche militaire. Cette ancienne dialectique de l'épée et du bouclier doit donc être prise en compte par les analyses de l'impact des technologies de sécurité hybrides. Loin de s'imposer de manière unilatérale sur des

[18] Le gouvernement canadien et l'Union Européenne sont engagés dans une démarche identique, qui vise à restructurer leurs initiatives de recherche et leurs industries des technologies de sécurité intérieure. En ce qui concerne le Canada, il s'agit de l'initiative *Security Clusters*, qui est conjointement piloté par le Centre Canadien de Recherches Policières et le Conseil National de Recherches Canada. Pour l'Europe, voir le communiqué de presse de la Commission Européenne IP/03/1351, daté du 7 octobre 2003.

[19] La métaphore de la constellation en sécurité intérieure est développée par Leman-Langlois (2002) et nous la reprenons ici dans le sens d'un groupe infini d'astres/acteurs isolés dans un espace en expansion.

[20] On notera d'ailleurs le caractère répétitif de la littérature sur la surveillance publique et les données éparses sur la déclinaison privée de ce phénomène.

citoyens ignorants de leur environnement et impuissants, elles font l'objet de résistances et de processus d'ajustement qui modulent leur efficacité objective et symbolique. Les organisations criminelles ou terroristes sont bien sûr celles qui mettent en œuvre ces stratégies et ces technologies de résistance de façon systématique : les cartels de la drogue colombiens ou les terroristes irlandais font par exemple usage des techniques d'analyse des réseaux sociaux et de logiciels de croisement des données afin d'identifier les informateurs en leur sein ou « pronostiquer » les opérations des services de police à leur encontre (Kailha 2002, van Meter 2002). La technologie militaire de changement aléatoire des fréquences, maintenant disponible dans les équipements de communication civils, est systématiquement utilisée par les trafiquants de drogue, rendant les interceptions difficiles, si ce n'est impossibles (Broad 2001). Les terroristes ou les « États voyous » peuvent télécharger sur Internet pour quelques dizaines de dollars des programmes qui calculent la trajectoire de milliers de satellites, y compris ceux appartenant à la communauté du renseignement américain[21].

Mais sans avoir recours à des technologies avancées, la simple connaissance des mécanismes de surveillance par ceux qui en font l'objet leur permet aisément de se soustraire à celle-ci. Les militants altermondialistes ou les opposants des régimes politiques autoritaires le savent bien, qui utilisent toute la panoplie des nouvelles technologies (téléphones cellulaires, courriel, SMS…) et les logiciels de cryptage des données disponibles gratuitement sur Internet pour tromper la vigilance des dispositifs de maintien de l'ordre. De même, la simple connaissance des paramètres de réglage des programmes de profilage censés alerter les responsables de la sécurité aérienne sur la dangerosité des passagers a permis aux terroristes du 11 septembre de passer sans encombre les contrôles. Ces derniers avaient en effet acheté leurs billets sur Internet avec plusieurs semaines d'avance à l'aide de leurs cartes de crédit, alors que les systèmes en place étaient programmés pour détecter des achats d'allers simples le jour du départ avec paiement en espèces. Nous pourrions encore continuer longtemps cet inventaire, mais les exemples déjà cités semblent suffisamment nombreux pour illustrer à quel point les techniques de contrôle peuvent être retournées contre leurs utilisateurs. Le déterminisme associé à la notion de militarisation des technologies de sécurité nous semble dans ce contexte mal évaluer la capacité des acteurs à exploiter les failles ou les atouts d'une technologie présentée comme oppressive, et minimiser le rôle joué par les ces mêmes technologies dans l'instauration d'une société plus ouverte et transparente.

Conclusion

Comme nous nous sommes employés à le démontrer, l'existence d'un mouvement de transfert technologique du secteur de la défense nationale vers celui de la sécurité intérieure, dont la conséquence principale serait l'érosion inéluctable des droits et libertés individuelles est une proposition séduisante qui reste cependant confrontée à un certain nombre de faits dont l'interprétation est sujette à discussion. On peut certainement identifier un mouvement de convergence entre la défense nationale et la sécurité intérieure, notamment par le biais de technologies partagées, d'efforts conjoints de recherche et de développement, ou de récupération pure et simple. Mais établir une relation causale directe entre cette convergence protéiforme et un resserrement du filet de contrôle social nous semble exagéré et injustifié tant que n'auront pas été menées des études empiriques additionnelles. Tout au plus peut-on parler d'une hypothèse de travail parmi d'autres sur une question qui reste sous-étudiée,

[21] Les deux logiciels les plus populaires dans la communauté des observateurs de satellites, qui alimentent de leurs données ces programmes sont *SatSpy* et *C-Sat*.

malgré ses implications pour la bonne santé démocratique de nos sociétés. Nous avons avancé dans ce chapitre quelques arguments mettant en question le caractère unidirectionnel et unidimensionnel de l'échange. Aux transferts de l'armée vers la police, on peut opposer des exemples de transferts inverses; à la rationalité purement technologique, on doit substituer un cadre pluriel de rationalités parfois convergentes, parfois concurrentes, dont le perpétuel réarrangement est imprévisible. Enfin, le caractère unificateur du cadre conceptuel utilisé par les tenants d'une société de surveillance maximale masque les réappropriations, les résistances et les détournements qui sont faits par une multitude d'acteurs des technologies mises à leur disposition par la logique exacerbée du marché. Si les enjeux soulevés par les défenseurs des libertés et les chercheurs qui se font leurs porte-parole sont d'une importance capitale, il nous semble que ces derniers succombent trop facilement à la même tentation que leurs adversaires, c'est-à-dire une réification des technologies de sécurité. Bien qu'il soit difficile d'échapper à une telle critique lorsqu'on cherche à interpréter et analyser l'impact des technologies de sécurité, une telle attitude ne peut qu'obscurcir un peu plus les termes d'un débat déjà passablement touffu.

Références

ABBATE J., 1999, *Inventing the Internet: Inside Technology*, MIT Press, Cambridge.

AMNESTY INTERNATIONAL, 2001, *Stopping the Torture Trade*, Londres.

BROAD W., 2001, « Surge in New Technologies Erodes US Edge in Spying », *The New York Times*, 20 septembre.

BRODEUR J.-P., 2003, *Les Visages de la Police*, PUM, Montréal.

BRODEUR J.-P. et LEMAN-LANGLOIS S., « La nouvelle surveillance : induction et déduction », article soumis aux *Cahiers de la Sécurité Intérieure*.

CASTELLS M., 2001, *L'Ère de l'Information : Tome 1, La Société en Réseaux*, Fayard, Paris.

CHAMBON F., 2002, « L'attribution de flash-balls à la police de proximité provoque une polémique », *Le Monde*, 18 mai 2002.

COATES J., 1970, *Nonlethal and Nondestructive Combat in Cities Overseas*, Institute for Defense Analysis, Alexandria.

DEPARTMENT OF DEFENSE et DEPARTMENT OF JUSTICE, 1994, *Memorandum of Understanding Between Department of Defense and Department of Justice on Operations Other than War and Law Enforcement*, DoD et DoJ, Washington DC.

DEPARTMENT OF DEFENSE, 2002, *Fiscal Year 2003 Budget Request*, DoD, Washington.

DICK P. K., 1956, « The Minority Report », *Fantastic Universe*, janvier. Ouvrage consulté : *The Minority Report: The Collected Stories of Philip K. Dick*, 2002, Citadel Press, Sacramento.

DUNLAP C., 2001, « The Thick Green Line : The Growing Involvement of Military Forces in Domestic Law Enforcement », in *Militarizing the American Criminal Justice System*, P. Kraska (dir.), Boston, Northeastern University Press, pp. 29-42.

DUNN T., 2001, « Waging a war on immigrants at the US-Mexico border », in *Militarizing the American Criminal Justice System*, P. Kraska (dir.), Boston, Northeastern University Press, pp. 65-81.

ELLUL J., 1988, *Le bluff technologique*, Hachette, Paris.

JANOWITZ M., 1960, *The Professional Soldier: a Social and Political Portrait*, Free Press, Glencoe.

HULSE C., 2003, « Congress Shuts Pentagon Unit over Privacy », *New York Times*, 25 septembre.

HUMAN RIGHTS WATCH, 1998, *Shielded from Justice: Police Brutality and Accountability in the United States*, HRW, New York.

KAILHA P., 2002, « The Technology Secrets of Cocaïne Inc. », *Business 2.0*, juillet.

LEMAN-LANGLOIS S., 2002, « The Myopic Panopticon : The Social Consequences of Policing Through the Lens », *Policing and Society*, Vol. 13, No. 1, pp. 43-58.

LOADER I., 1999, « Consumer Culture and the Commodification of Policing and Security », *Sociology*, Vol. 33, No. 2, pp. 373-392.

MANNING P. K., 2001, « Technology's Ways: Information Technology, Crime Analysis and the Rationalizing of Policing », *Criminal Justice*, Vol. 1, No. 1, pp. 83-103.

MANNING P. K., 2003, *Three Modes of Security*, document de travail non publié, Boston.

MARX G. T., 2001, « Technology and Social Control : The Search for the Illusive Silver Bullet », in Smelser N. et Baltes P. (eds.), *International Encyclopedia of the Social and Behavioral Sciences*, http://www.sciencedirect.com/science/article/B6WVS-46RR9GP-7/2/15dcb0adb4d56e88d1b89288a7d4f8ea.

MARX G. T. et CORBETT R., 1991, « Critique : No Soul in the New Machine : Technofallacies in the Electronic Monitoring Movement », *Justice Quarterly*, Vol. 8, No. 3, pp. 399-414.

MOSKOS C., 1975, « The Constabulary Ethic and Military Professionalism », *Armed Forces and Society*, Vol. 1, No. 4, pp. 388-401.

MURPHY V., 2001, « Spook Valley », *Forbes Magazine*, 12 novembre.

NEWBURN T., 2001, « The Commodification of Policing: Security Networks in the Late Modern City », *Urban Studies*, Vol. 38, No. 5-6, pp. 829-848.

NOLLINGER M., 1995, « Surrender or we'll slime you », *Wired Magazine*, No. 3.02, p. 17-22.

ORWELL G., 1980, *1984*, Gallimard, Paris.

PINSKER B., 2003, « Confessions of a baggage screener », *Wired Magazine*, No. 11.09, p. 86-88.

SAUTENET V., 2000, Legal Issues Concerning Military Use of Non-Lethal Weapons, *Murdoch University Electronic Journal of Law*, Vol. 7, No. 2, accessible à http://www.murdoch.edu.au/elaw/issues/v7n2/sautenet72_text.html

SEASKATE INC., 1998, *The Evolution and Development of Police Technology*, National Committee on Criminal Justice Technology, Washington DC.

SERVICE DE POLICE DE LA COMMUNAUTÉ URBAINE DE MONTRÉAL, 2001, *Bilan Annuel 2000*, SPCUM, Montréal.

SINISCALCHI J., 1998, *Non-Lethal Technology: Implications for Military Strategy*, Center for Strategy and Technology, Maxwell Air Force Base.

STANLEY J. et STEINHARDT B., 2002, *Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida*, ACLU, New York.

VAN METER K. M., 2002, « Terrorists/Liberators : Researching and Dealing with Adversary Social Networks », *Connections*, Vol. 24, No. 3, pp. 66-78.

WRIGHT S., 1998, *An Appraisal of Technologies for Political Control*, Luxembourg, Parlement Européen.