LA SURVEILLANCE TOTALE

Par Jean-Paul Brodeur et Stéphane Leman-Langlois
Centre international de criminologie comparée
Université de Montréal

Texte publié dans Cahiers de l'IHESI, N° 55, 61-90.

INTRODUCTION

Après les attentats du 11 septembre 2001, le Congrès des Etats-Unis institua une enquête parlementaire sur les services de renseignement, accusés d'avoir failli à leur tâche de prévenir ces attentats. L'enquête fut effectuée de façon conjointe par la Chambre des représentants et le Sénat de ce pays (United States, Congress, 2002). Le vice-président du comité Sénatorial — le sénateur Richard B. Shelby — soumit en outre un rapport additionnel, qui faisait état des investigations qu'il a lui-même conduites dans les marges de l'enquête du Congrès (Shelby, 2002). Ces rapports se sont accompagnés d'une dénonciation par un agent du *Federal Bureau of Investigation* (FBI) — Coleen Rowley — de l'incurie des cadres du FBI (Rowley a été désignée *Person of the Year* par l'influent *Law Enforcement News*; voir Nislow, 2002).

Pris ensemble, ces écrits ne présentent pas seulement une critique sévère de la « communauté du renseignement » des Etats-Unis, mais ils constituent une anti-mythologie des appareils de surveillance qui opèrent dans ce pays et nous révèlent à quel point nous connaissons mal ce dispositif (sur ce sujet, voir Québec, 1981). La représentation des appareils de surveillance qui y est élaborée ne s'applique pas seulement aux Etats-Unis mais aussi au Canada, dont le cas de figure apporte une confirmation additionnelle aux révélations des enquêtes étatsuniennes. Dans ce texte, nous traiterons d'abord des changements qui ont été apportés aux appareils de surveillance au Canada et nous nous pencherons ensuite sur la situation étatsunienne. Dans les deux cas, nous réfléchirons sur la surveillance effectuée au moyen d'une technologie de plus en plus proliférante. En conclusion, nous énoncerons quelques-uns des traits qui caractérisent cette nouvelle surveillance.

1. L*E CANADA ET LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS*

Commençons immédiatement par dissiper un malentendu si répandu qu'on en trouve la manifestation dans un film comme *Bowling for Columbine* de Michael Moore. Pour l'essentiel, ce malentendu consiste à voir dans le Canada le pays de la civilité et de la mesure, en comparaison des excès en tout genre qu'on trouve aux Etats-Unis. Or, la mesure canadienne n'est pas partout évidente. En 2002, par exemple, les tribunaux étatsuniens ont accordé 1 491 autorisations de procéder à l'interception de communications privées, une augmentation de 24% par rapport aux quelque 1 200 permissions annuellement accordées par les juges des Etats-Unis (*Law Enforcement News*, 2002 : 13). D'après nos recherches, les tribunaux canadiens ont accordé 14 304

autorisations de cette nature de 1974 à 1998, ce qui constitue une moyenne d'environ 600 mandats d'écoute électronique par année, sans compter les mandats décernés dans le cadre de la protection de la sécurité nationale du Canada. Comme la population du Canada est dix fois moins nombreuse que celle des Etats-Unis, on y pratique donc proportionnellement l'écoute électronique cinq fois plus fréquemment qu'aux Etats-Unis. L'Australie pratique également l'écoute électronique plus fréquemment que les Etats-Unis et, fait notable, les projets d'écoute électronique dans ce pays conduisent proportionnellement beaucoup mois souvent à des accusations criminelles portées contre ceux qui en sont la cible qu'aux Etats-Unis.

Dans la suite des attentats de septembre 2001, le Canada s'est livré à une intense activité législative, promulguant plusieurs lois et transformant en 2004 son ministère du Solliciteur général en ministère de la « Sécurité publique et de la Protection civile ». Depuis décembre 1999 le Canada était sous les feux de la critique de son voisin du sud pour n'être pas intervenu contre Ahmed Ressam, un terroriste qui fut intercepté à la frontière étatsunienne, à la veille de perpétrer un grave attentat lors des célébrations saluant le passage au nouveau millénaire. L'incurie des services canadiens de renseignement dans cette affaire avait en effet été flagrante.

La première et la plus importante des nouvelles législations fut le Projet de loi C-36, promulgué par le Parlement canadien en 2002 sous le nom de *Loi antiterroriste*. C'est sur cette loi d'une grande complexité (plus de 200 pages de texte), élaborée dans la hâte et adoptée sans consultation, que nous nous pencherons d'abord.[1]

Bien que son histoire remonte au lendemain de la Première guerre mondiale, le Centre de la sécurité des communications du Canada (CST) fut créé sous son nom actuel par un décret du pouvoir exécutif en 1975 (décret PC 1975-95). Il exerçait toutefois toutes ses fonctions depuis 1947, dans le cadre du traité UKUSA, dont les États-Unis, la Grande-Bretagne, l'Australie, la Nouvelle-Zélande et le Canada sont les signataires (pour une histoire du CST, voir Brodeur, 2003). Comme la *National Security Agency* (NSA) aux Etats-Unis, le *Government Communications Headquarters* (GCHQ) au Royaume-Uni et, plus récemment, la Direction du renseignement militaire en France (DRM), le CST est un *service de renseignement* qui utilise une technologie très puissante pour intercepter une grande variété de signaux électroniques (radio, téléphone, télévision, internet). Les données ainsi recueillies sont analysées par les ordinateurs les plus puissants dont on disposait jusqu'à récemment (des ordinateurs de marque Cray). La mission du CST est de protéger la sécurité nationale du Canada. Elle est donc avant tout politique et ne relève pas directement de l'application des lois pénales du Canada. Comme ceux de la NSA, les budgets du CST dépassent largement ceux des services traditionnels de renseignement, qui exploitent plutôt des sources humaines (HUMINT) que des sources techniques (SIGINT). Dans l'après-septembre 2001, le gouvernement canadien a octroyé au CST plus des trois quarts des budgets

1) L'un des auteurs de ce texte — Jean-Paul Brodeur — a été convoqué comme témoin expert par le comité parlementaire chargé d'examiner le projet de loi. Il a reçu le texte très élaboré de cette loi deux jours avant de témoigner devant le comité. Il a refusé de s'y présenter, cette consultation étant de pure forme.

d'urgence alloués aux divers services de renseignement.

Il importe toutefois de souligner qu'à la différence du Service canadien de renseignement de sécurité (SCRS), le CST ne disposait pas, jusqu'à récemment, d'une loi qui déterminait son mandat, ses pouvoirs et sa redevabilité (*accountability*). Comme son homologue étatsunien, la NSA, le CST opère depuis 1947 de façon plus ou moins officieuse, sous l'autorisation de décrets du pouvoir exécutif[2]. Par suite de pressions de l'opinion publique, le CST est depuis 1996 supervisé par un commissaire — le Commissaire du Centre de la sécurité des télécommunications. Le premier commissaire qui a été nommé par le gouvernement est l'ancien juge en chef de la Cour d'appel du Québec, le juge Claude Bisson, qui est toujours en fonction. Le juge Bisson a publié cinq rapports annuels entre 1996 à 2001. Ces rapports comportent un leitmotiv : dans presque chacun d'eux, le Commissaire émet le vœu que le CST soit encadré par une « loi d'habilitation ». De plus, chaque fois qu'il a émis ce souhait, il a toujours insisté sur la nécessité de soumettre le contenu de cette loi d'habilitation à une vaste consultation et à un débat public. Or, c'est très précisément ce que le gouvernement a évité de faire. Un peu à la manière d'un cheval de Troie, on trouve dans un recoin de la Loi antiterroriste l'équivalent d'une loi d'habilitation du CST en bonne et due forme. C'est à dessein que nous utilisons l'expression de cheval de Troie. En effet, il se trouve enfoui dans le ventre de cette loi d'habilitation, qui n'a fait l'objet d'aucun débat public avant son dépôt, un accroissement significatif des pouvoirs du CST.

Avant la loi d'habilitation introduite de façon subreptice par le projet C-36, le mandat du CST consistait en deux volets:

— Premier volet : l'interception de communications de toute nature dirigées vers l'étranger, en provenance de pays étrangers vers le Canada ou échangées entre deux pays étrangers. Il faut souligner qu'en principe le CST n'intercepte pas les communications des Canadiens ou des immigrants reçus. Il peut toutefois arriver que dans un faisceau d'ondes électroniques interceptées d'un seul coup se trouvent des communications échangées entre des Canadiens. Dans ce cas, elles sont en théorie extraites de l'ensemble et effacées. Le Commissaire du CST nous en a redonné l'assurance dans chacun de ses rapports et il n'y a pas de raison de mettre ses assurances en doute.

— Deuxième volet : si le premier volet est agressif, le second est défensif. Le CST a pour mission de protéger le système de communication du gouvernement du Canada contre toute forme d'intrusion, de déstabilisation et d'interception de la part d'un pays étranger.

Tel était donc le mandat du CST jusqu'au dépôt du projet de loi C-36. Celui-ci repris les deux premiers volets du mandat ci-haut énoncé. Il ajouta toutefois un énigmatique troisième volet:

> *fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère* (article 273.64 (1) c)).

2) Les Étatsuniens disent avec humour que le sens de l'abréviation « NSA » est « No Such Agency (exists) » (une telle agence n'existe pas).

La question que l'on doit se poser est bien sûr : « qu'est-ce que cela signifie? ». Précisons d'abord qu'en langage juridique « les organismes fédéraux chargés de l'application de la loi » (*law enforcement*) sont les corps de police, au premier chef la Gendarmerie royale du Canada. L'organisme responsable de « l'application […] de la sécurité » au sens politique du terme est le SCRS. De façon plus particulière, est-ce que le texte cité plus haut permettra l'interception des communications privées des Canadiens sans leur consentement? Ces questions sont redoutables et nous avons communiqué avec le personnel du bureau du Commissaire du CST, afin d'en apprendre davantage. Le personnel du Commissaire a été accueillant et nous a renseigné, en demeurant dans le cadre de ses obligations de confidentialité, exigées par la sécurité nationale du Canada.

Voyons comment l'ajout au mandat du CST se traduit dans la pratique, à partir de deux exemples particuliers :

— Premier exemple : un service de police ou le SCRS pourraient intercepter légalement une communication encodée ou venir en possession d'un objet, par exemple un CD-ROM, également encodé. Comme le CST comporte du personnel spécialisé dans le décryptage des codes (ce fut historiquement sa fonction originelle), les policiers ou le SCRS pourraient avoir recours à son service. Pourvu que les communications encodées n'aient pas été échangées entre des Canadiens, il n'y a là aucune difficulté.

— Deuxième exemple (plus problématique) : la Loi antiterroriste affirme que si le CST procède à l'interception de communications entre des Canadiens, il sera assujetti aux mêmes limites que la loi impose aux corps policiers et au SCRS en relation avec ce type d'interception. En clair, cela signifie qu'il devrait jouir d'une autorisation judiciaire pour intercepter les communications privées. Comme le CST est en position d'assistance à un autre service — le SCRS ou un corps policier — ce sont donc ces services qui feront la demande d'interception auprès d'un magistrat. La question cruciale est alors celle-ci : est-ce que la demande présentée au magistrat mentionnera le rôle du CST dans l'interception? Nous avons explicitement posé cette question au personnel du Commissaire du CST et obtenu une double réponse. D'abord, que la question est tout à fait pertinente (comme on nous a dit en anglais « *You are right on the money!* » — « Vous avez mis dans le mille! »). Ensuite, que la réponse à cette question ne peut être fournie pour des raisons de protection de la sécurité nationale du Canada.

On peut conclure de ces hésitations qu'un problème risque effectivement de se poser. Il n'est pas déraisonnable de penser que le passage que nous avons cité implique que le CST pourrait se mêler d'intercepter les communications privées des Canadiens. Cependant, si nous nous en rapportons à la réponse qui a été fournie aux questions relatives à notre second exemple, on ne sait trop à quel point sera divulguée l'implication du CST dans l'interception des communications privées des Canadiens. En d'autres termes, sera-t-il soumis dans ses tâches d'assistance aux services policiers avec les mêmes exigences de redevabilité que ces derniers, ainsi que la Loi antiterroriste semble l'affirmer, tout en cultivant délibérément l'ambiguïté? Nous ne pouvons à l'heure présente répondre à cette question, dont on a reconnu la pertinence.

Le cas de figure canadien révèle deux évolutions significatives, à la suite des attentats du 11 septembre 2001.

— D'abord, le dispositif mis en place donne une forte priorité à la surveillance technologique (SIGINT) aux dépens de la surveillance plus traditionnelle qui est exercée par des fonctionnaires de police et leurs agents (HUMINT).

— Ensuite, on tente de favoriser un rapprochement entre les services de renseignement qui, pour l'essentiel, se consacrent à la surveillance des ressortissants étrangers et les forces policières, dont les interventions s'exercent sur tous les délinquants sans distinction légale (ou autrement institutionnalisée), ainsi qu'entre les menaces provenant de l'intérieur du territoire national et celles qui sont générées par l'action d'un État ou d'une organisations étrangers.

Comme nous le verrons dans la suite, ces développements se sont produits à plus grande échelle aux Etats-Unis, où ils ont pris une importance exemplaire.

2. *LES ÉTATS-UNIS ET LE PROJET « TOTAL INFORMATION AWARENESS »*

Il faut commencer par rappeler que deux des services de renseignement étatsuniens — la composante politique du *Federal Bureau of Investigation* (FBI) et la *Central Intelligence Agency* (CIA) — ont fait l'objet de nombreuses controverses. En effet, plusieurs comités du Congrès des États-Unis ont passé au peigne fin les milieux du renseignement étatsuniens à la suite du scandale du Watergate qui éclata au début des années 1970. L'enquête la plus approfondie fut effectuée par le comité spécial du Sénat sur les activités des services de renseignements et de sécurité (*Senate Select Committee on Intelligence Activities*), présidé par le sénateur de l'Idaho, M. Frank Church. Le rapport du comité exposait en détail les opérations menées à l'intérieur du pays par le FBI contre les dissidents politiques dans le cadre de son notoire programme de contre-espionnage (*Counter Intelligence Program* — COINTELPRO — dont furent victimes Martin Luther King et l'actrice Jean Seberg); il se penchait également sur les opérations clandestines de la CIA à l'extérieur du pays (US Congress, 1976, le Rapport Church; voir aussi, US Congress, 1977, le Rapport Pike).

À la suite de ces rapports, le FBI et la CIA durent se réformer en profondeur. Or, dans sa critique sévère de l'échec des services de renseignement à prévenir les attentats du 11 septembre 2001, le sénateur Shelby attribue en partie leur contre-performance à la situation qui a été engendrée par ces réformes (Shelby, 2002). Cette situation s'est mise en place à la suite de la volonté des services de respecter deux exigences relevant de l'obligation de moyen et dont les conséquences au plan de l'obligation de résultat ont été estimées désastreuses par Shelby et ses collègues du Congrès.

La première de ces exigences était de respecter la vie privée des citoyens étatsuniens. Aux États-Unis, les opérations de surveillance *intérieure* du territoire sont pour l'essentiel encadrées par le *Foreign Intelligence Surveillance Act* (FISA, proclamé en 1978) qui, comme son nom l'indique, ciblait exclusivement les *étrangers* (« *non US persons »)* soupçonnés de se livrer à des activités nuisibles à la sécurité des États-Unis. On résolut donc l'aporie d'exercer une surveillance politique sur les Étatsuniens sans envahir leur vie privée de manière radicale en limitant la surveillance aux étrangers résidant sur le territoire des Etats-Unis. Cette scission initiale entre le renseignement

politique sur les étrangers et le renseignement policier sur les Étatsuniens devait engendrer une culture sectaire du renseignement caractérisée par le refus intransigeant de partager l'information et au cloisonnement rigide des opérations effectuées par les diverses composantes de l'appareil de surveillance.

Ce sectarisme empêcha les autorités étatsuniennes d'intercepter deux des kamikazes qui ont participé aux attentats de septembre 2001. Ces deux terroristes — Khalid Al-Mihdhar et Nawaf Al-Hazmi — furent repérés par les services de renseignement de la Malaisie, lorsqu'ils assistèrent à une réunion où se trouvaient des membres d'Al Qaida, à Kuala Lumpur, au début de janvier 2000. Cette information fut transmise à la CIA et à la NSA, qui surveillaient déjà indépendamment ces deux individus. Il existe aux États-Unis un programme appelé TIPOFF (prévenir), selon lequel les services de renseignement *doivent* soumettre aux services d'immigration et aux agences consulaires accordant des visas une liste de noms d'individus soupçonnés d'activités terroristes et dont la présence n'est pas désirable aux États-Unis. Néanmoins la CIA se refusa obstinément à mettre Al-Midhar et Al-Hazmi sur une liste de surveillance, bien qu'elle eût appris en janvier 2001 qu'ils étaient liés à un terroriste qui avait participé à l'attentat contre le destroyer USS Cole, au Yémen. Il y eut même des échanges informels entre le FBI et la CIA sur ces deux personnes, la CIA assurant le FBI que celles-ci étaient à l'extérieur du territoire des États-Unis, même si elle savait cette information fausse. En effet, de janvier 2000 à septembre 2001, ces deux terroristes vécurent à San Diego sous leur propre nom — l'un d'eux était même inscrit dans l'annuaire téléphonique de cette ville — et prirent en mai 2000 des leçons de vol dans une école de pilotage étatsunienne. Comme ils s'absentaient assez fréquemment des États-Unis, ils devaient renouveler leur visa et repasser les frontières. On disposait donc de plusieurs occasions de les intercepter, si leur nom avait été transmis aux autorités compétentes, en conformité ave le programme TIPOFF. La CIA ne se résolut à les signaler à TIPOFF *qu'à la fin d'août 2001*. Il était alors trop tard, car ils étaient revenus aux États-Unis et s'affairaient aux derniers préparatifs des attentats de septembre. Le 11 de ce mois, ils faisaient partie du commando qui précipita un avion d'*American Airlines* sur le Pentagone. Un cloisonnement horizontal étanche entre les diverses banques de renseignement ôta toute chance aux services concernés de faire des arrestations qui auraient pu conduire à la découverte du complot.

Ce cloisonnement horizontal entre les diverses sources d'information s'est prolongé dans une fracture verticale entre le renseignement et son utilisation. En effet, les scandales reliés aux opérations politiques de déstabilisation (*disruptive tactics*) du FBI et de la CIA (*covert operations*) dans les années 1970 donnèrent naissance à la seconde des exigences auxquelles nous nous sommes référés plus haut : le premier but de la surveillance politique doit être de recueillir des renseignements et non d'effectuer des opérations de neutralisation. Cette priorité, enchâssée dans la loi FISA, allait être progressivement interprétée par les tribunaux étatsuniens comme exclusive et limitant la surveillance politique à la cueillette de renseignements. C'est sur cette limitation que s'édifiera ce qu'on appelle aux Etats-Unis la « muraille de Chine » (*the wall*) entre les services de renseignement, qui accumulent des informations, et les forces policières, qui répriment la criminalité (Brodeur, 2000).

On mesurera la hauteur de la muraille à partir de l'affaire Zacharias Moussaoui. Celui-ci fut arrêté quelques semaines avant les attentats de septembre 2001, à cause de son comportement suspect dans une école de pilotage. Alors qu'il était en détention, des agents du FBI songèrent d'abord à obtenir un mandat pour fouiller ses affaires et examiner le contenu de son ordinateur *dans le cadre d'une enquête judiciaire* sur un crime de droit commun. Leurs chefs interdirent cette approche, car elle risquait de nuire à leurs démarches subséquentes pour obtenir un mandat en vertu de la loi FISA, qui est la loi de référence dans la lutte contre le terrorisme. La répression du crime de droit commun et celle de la délinquance politiquement motivée étant des domaines séparés, les opérations dans un champ ne doivent pas « contaminer » celles exécutées dans l'autre et vice-versa (Shelby, 2002 :51). Ils tentèrent donc d'obtenir leur mandat en vertu de la loi FISA, pour se faire répondre par les experts juridiques du FBI qu'ils devaient d'abord démontrer son affiliation avec l'une ou l'autre des organisations terroristes répertoriées par le ministère des Affaires étrangères. En dépit de leurs efforts, ils n'y parvinrent pas à temps pour prévenir les attentats du 11 septembre.

L'une des conséquences les plus funestes de ce divorce entre le renseignement et les opérations est le fossé qu'il creuse entre ce qui relève de l'analyse de l'information et ce qui appartient à l'intervention sur le terrain. Les agents qui opèrent sur le terrain sont les mieux informés dans leur secteur en raison de leur proximité de l'événement mais ils sont incapables de mettre les donnéés dont ils disposent en relation avec celles que possèdent d'autres intervenants, tant à cause de leur isolement que de leur manque de compétence dans le traitement de l'information. D'autre part, les analystes possèdent les ressources pour croiser les informations et relier les pointillés mais ils ne sont pas alimentés par les intervenants sur le terrain, en vertu du cloisonnement entre l'analyse stratégique et la tactique d'intervention. Pour paraphraser la célèbre formule de Kant, des analyses qui ne sont pas nourries par les opérations sont vides et des opérations qui ne sont pas guidés par l'analyse sont aveugles.

Les membres de la commission qui s'est penchée sur ces problèmes les estiment tellement profonds qu'ils doutent de la capacité des diverses composantes des appareils de surveillance de les résoudre. C'est pourquoi ils proposent la création de nouvelles structures, ainsi qu'un recours massif à la technologie pour effectuer un croisement des informations que les personnels refusent de partager. Nous allons maintenant examiner l'une des structures que l'on a tenté de développer pour résoudre le problème, la *Total Information Awareness* (vigilance information totale).

Aujourd'hui disparue sous les attaques généralisées dénonçant son énorme potentiel de grossières violations du droit à la vie privée, la TIA n'en reste pas moins un puissant exemple de solution technologique au problème du renseignement de sécurité dans un contexte policier. Par ailleurs, comme nous le verrons, bien que le programme TIA soit mort et enterré ses technologies et expertises ont été récupérés ailleurs.

A. *Contexte général*

L'*Information Awareness Office* fut créé comme l'un des deux principaux programmes de renseignement à la *Defense Advanced Research Projects Agency* (DARPA) du ministère de la Défense, le second étant le *Information Exploitation Office* (IXO). L'IXO

se concentre sur la production de renseignement, surtout au niveau de la problématique de la conduite des opérations sur le champ de bataille et produit des systèmes de dissémination d'informations sur l'évolution de situations stratégiques en temps réel. Remarquons immédiatement que le couple IAO/IXO témoigne d'une conscience aiguë de la nécessité de procéder à une intégration verticale du renseignement. John Poindexter, le directeur de l'IAO et ancien conseiller en sécurité nationale du président Reagan (où il avait participé au scandale Iran-Contras), proposa l'idée de développer ce programme au Pentagone quelques semaines après les attaques du 11 septembre 2001.

Bien que le Pentagone ait cité un budget de 10 millions USD pour l'IAO, son budget réel est apparemment bien plus élevé, soit quelque 245 millions pour l'année fiscale 2002-2003 — le chiffre de 10 millions ne comprenant aucun des sous-programmes de développement technologique impliqués. Il est à noter que la DARPA/IAO fait peu du travail par elle-même, la plupart des éléments du système étant confiés à l'entreprise privée, comme la compagnie pour laquelle Poindexter travaillait avant de devenir directeur de l'IAO (Syntek) ou comme la firme Booz Allen Hamilton, dont le vice président, Mike O'Connell, est un ancien directeur de la NSA.

Formé en janvier 2002, l'IAO n'a fait son entrée officielle dans les médias qu'en novembre 2002. La réalisation de son programme — le développement d'une technologie informatique de croisement du renseignement — était alors prévue pour 2005–2006; date où en principe les systèmes mis au point auraient pu être prêts pour une utilisation réelle par des agences de renseignement. Bien que développé par le Pentagone, le produit final *Total Information Awareness* n'était pas sensé être réservé aux militaires, ni à un usage dans le champ de la sécurité extérieure. En se référant aux bénéficiaires du programme, le site de l'IAO utilise d'ailleurs le mot « *warfighters* » plutôt que « *soldiers* », ce premier mot comprenant les employés de forces policières, en particulier le FBI, qui sont engagés dans la « guerre contre le terrorisme ». Notons donc le souci d'intégration horizontale.

Comme nous l'avons déjà mentionné, la principale pierre d'achoppement du projet se révéla être ses multiples niveaux de conflit avec les lois protégeant la vie privée. Ceci, malgré l'affaiblissement de plusieurs garanties juridiques déjà causé par le *Homeland Security Act*, ratifié en novembre 2002 par le Congrès. De plus, il faut noter que le *Cyber Security Enhancement Act*, enchâssé dans la loi créant le nouveau ministère de l'Intérieur, permet aux autorités d'obtenir des informations au sujet d'utilisateurs d'internet conservées par leur fournisseur de services et facilite l'installation d'instruments permettant la surveillance du courrier électronique (*pen registers* et *trap and trace devices*, comme le système « carnivore » mis au point par le FBI). Autre exemple, la section 215 du *USA Patriot Act* oblige déjà les libraires et les bibliothécaires à fournir au FBI des renseignements sur les habitudes de lecture de leurs clients, quand un agent de ce service a obtenu l'autorisation judiciaire requise. Qu'il ait été perçu comme une attaque contre les droits civiques pires que toutes ces dernières, ou simplement comme la goutte qui fit déborder le vase, l'IAO et sa TIA déclencha dans la presse et dans les milieux politiques une réaction qui finit par le retrait de son budget en octobre 2003 (S.1382, *Department of Defense Appropriations Act, 2004*, section

8120).

B. *Objectifs visés*

Bien que cet objectif paraisse contradictoire, l'IAO proposait de créer un « Big brother » qui serait respectueux de la vie privée des États-suniens. En fait, plutôt que de laisser des humains espionner les citoyens, il s'agissait de mettre en réseau des machines qui le feraient, dans la plus grande discrétion. Les surveillants humains n'intervenant que dans les cas où des *terroristes authentiques* seraient débusqués (« des méthodes automatisées améliorées de protection de la vie privée seront développées pour préserver l'identité de ceux dont les dossiers seront examinés par les logiciels de surveillance des flux de données »; ancien site de l'IAO, notre traduction). Le principe de base est que la lecture et l'analyse de la vie privée ne constituent pas des intrusions si elles sont effectuées par une machine. Entre autres raisons, parce qu'une machine peut être programmée pour ne garder en mémoire que les informations estimées pertinentes par son programmateur et dont la cueillette est autorisée par la loi. Il n'en va pas ainsi de la surveillance exercée par les humains, qui ne peuvent à leur gré chasser de leur mémoire les informations qui n'auraient pas dû y entrer. Par exemple, un policier qui se livre à l'écoute électronique ne peut éviter de retenir tout un ensemble d'informations sur la vie intime de ceux dont il écoute les conversations, même s'il sait que ces informations sont dénuées de pertinence pour son enquête. Comme Edwy Plenel l'a remarqué, c'est de savoir qu'on a été espionné dans ses replis — par exemple, les vacances, les maladies des enfants ou leurs résultats scolaires — qui est le plus intolérable (Plenel, 1997 : 299-314). En d'autres termes, la machine peut fonctionner de manière rigoureusement sélective, alors que le surveillant humain ne peut opérer que de manière totalisante. Le recours à la surveillance informatisée implique toutefois un changement encore plus profond.

Le concept de base est de créer un système modulaire entièrement automatisé permettant de draguer du flux des données (*data mining*) toutes les informations pour construire des *patterns* (séquences types ou événements-clés) révélateurs d'activité terroriste et, surtout, proto-terroriste, afin d'en prévenir l'occurrence. En principe le système devait être capable d'avertir les analystes qui en feront l'utilisation moins d'une heure après qu'un événement-clé se serait produit quelque part.

Le système prévu était formé de trois composantes. La première de celles-ci est de nature analytique. Des *patterns* exemplaires devaient être extraits de l'analyse d'une base de données contenant 90 % des actes terroristes internationaux. Les actions terroristes avaient été segmentées en un ensemble d'activités ou « transactions » — par exemple, la demande d'un passeport, celle d'un visa, l'utilisation d'une carte de crédit, la demande d'un permis de travailler ou d'un permis de conduire, l'achat de billets d'avion, la location d'une voiture, l'achat de produits chimiques, d'armes, l'entreprise de divers apprentissages (des leçons de pilotage ou de plongée sous-marine) et un nombre encore inconnu d'autres transactions sur des banques de données diverses; à ceci s'ajoutaient évidemment les informations contenues dans les bases de données des services de renseignement policiers et de sécurité ainsi que les informations détenues par la justice pénale sur les arrestations, les condamnations, les peines et les

élargissements. C'est à partir de cette masse de données qu'on avait commencé à constituer un répertoire de séquences-type (*patterns*) annonciatrices d'un attentat prochain (voir la conférence de presse du sous-ministre de la Défense, Peter Aldridge, le 20 novembre 2002 : http://irregulartimes.com/iaoinfo.html).

La seconde composante du système était de nature transactionnelle : il s'agissait de surveiller en continu les transactions effectuées dans un grand nombre de domaines. Les domaines retenus par l'IAO en 2002 étaient très nombreux et concernaient les champs suivants : finances, éducation, déplacements, médecine des hommes et des animaux, la passage des frontières, les transports publics, le logement, les services (gaz, eau, électricité), le gouvernement et les communications (selon l'ancien site de l'IAO, maintenant disparu : http://www.darpa.mil/iao/TIASystems.htm).

La troisième composante, en relation potentielle avec la seconde , relevait de l'identification des personnes et impliquait la collecte et l'analyse de diverses données biométriques (faciès, démarche, empreintes génétiques, digitales, oculaires, et autres données permettant de produire et de confirmer une identification).

Le fonctionnement du système peut être illustré de la manière suivante (l'exemple est délibérément simple pour les besoins de cet article). Imaginons que la composante analytique comporte la séquence-type suivante : achat d'un billet d'avion dans un aéroport, peu de temps avant le décollage de l'avion, avec paiement en espèces et date de retour du voyageur laissée indéterminée. Supposons en outre que le monitoring des transactions effectuées dans le domaine du transport aérien révèle l'occurrence effective d'une telle séquence. Une alerte sera alors lancée et les opérateurs du système tenteront d'utiliser sa composante d'identification pour retracer l'auteur de la transaction, qu'on soumettra dans les plus brefs délais à une arrestation préventive. L'information recueillie par le monitoring automatisé des transactions n'est donc pas en théorie utilisée avant qu'une séquence-type ou un événement déclencheur aient été détectés; le renseignement personnel qui n'est pas relié à une activité terroriste continue de faire partie du « bruit de fond » (*noise*) de la base de données et n'est connu que de la machine.

C. *Instruments préconisés*

La TIA comprenait plusieurs sous-programmes, chacun avec son budget indépendant à la DARPA. D'ailleurs, une des principales tâches de l'IAO était l'intégration progressive de technologies variées et à divers stades de complétion. Une seconde tâche, d'une complexité qu'on ne saurait sous-estimer, tenait dans la mise en réseau de sources de données très hétéroclites. Sans compter le défi politique d'obtenir les autorisations du pouvoir exécutif et, éventuellement, des tribunaux, nécessaires à la mise en commun de données protégées par les lois sur la vie privée. Voici quelques uns des sous-programmes développés sous l'égide de l'IAO, dont la plupart existent toujours sous une

3) De façon significative, le lien entre ces deux composantes était représenté sur un des organigrammes de la DARPA par une chaîne dont l'un des maillons est brisé, ce qui indique que la mise en relation de ces deux composantes s'effectuerait selon un protocole sélectif prédéterminé. Cet organigramme a été supprimé au début 2003 car le répertoire des banque de données qu'il contenait était trop inquiétant pour l'opinion publique.

forme ou une autre à l'extérieur de la DARPA :

— *HumanID* : *Human Identification at a Distance*. HID est le descendant direct du programme FERET (*Face Recognition Technology*) créé en 1993 par le *Counterdrug Technology Development Program Office* (CDTDPO; programme militaire de lutte contre le trafic de stupéfiants) du ministère de la Défense (*Department of Defense, DoD*). Le programme vise à développer les technologies de reconnaissance des visages humains *à distance*. Contrairement à des systèmes existants servant de clef d'entrée, où le visage de l'utilisateur est placé à un endroit précis pour fins d'identification, HumanID vise l'analyse instantanée de visages dans les foules et dans les endroits publics — en temps réel ou en analyse différée de documents visuels préexistants. Cet outil appartient donc à la troisième des composantes du système (l'identification).

— *Genisys*. Le programme Genisys poursuivait quatre objectifs. Le premier était de nature essentiellement quantitative : on voulait procéder à un élargissement très important de la nature et du volume des informations recueillies, analysées et conservées au sein de la super-banque de données de la TIA. Le second tenait à la mise en forme de ces données : on se proposait de formater toutes ces données de manière simple et uniforme, de manière à ce qu'elles soient facilement accessibles aux services étatsuniens concernés et, potentiellement, à ceux des alliés des États-Unis. Le troisième visait à augmenter la qualité des données en spécifiant les paramètres d'espace et de temps où elles s'insèrent, permettant ainsi de réduire l'incertitude que comporte leur utilisation. Finalement, le programme poursuivait un ambitieux objectif normatif : on lui aurait adjoint des filtres permettant de dé-nominaliser les données, en remplaçant, par exemple, les noms des personnes par des alias, de telle sorte que le système protège la vie privée de la masse des citoyens qui ne sont pas impliqués dans le terrorisme.

— *TIDES* (*Translingual Information Detection, Extraction and Summarization*). Tides permettra aux analystes de comprendre des communications faites dans des langues étrangères. Le portugais, le français, l'italien, l'allemand, le russe et l'espagnol sont déjà intégrés au système. Le programme se concentre maintenant sur le mandarin et l'arabe. Ce programme a survécu à la disparition de l'IAO/TIA et reste en développement.

— *Babylon*. Version portable de TIDES, disponible sur ordinateur de poche et permettant la traduction immédiate de différents langages sur le terrain. Cette technologie est déjà utilisée en Afghanistan depuis le printemps 2002, à titre de projet-pilote. Sa fonction au sein de la stratégie TIA n'est pas claire et semble à première vue superflue. Cependant, il faut noter qu'il existe également un sous-programme appelé *Communicator*, qui permettra de converser avec un ordinateur; il est possible que la conjonction des deux instruments vise à permettre l'intégration et l'analyse sémantique en temps réel des conversations dans le cadre d'opérations militaires ou en interface avec Genisys pour la détection sur le terrain de *patterns* terroristes.

— *EARS* (*Effective, Affordable, Reusable Speech-to-Text*). On cherchait ici à développer une solution de transcription automatique de conversations parlées. Les documents écrits sont ensuite intégrés à Genisys.

— *Bio-Surveillance*. Ce programme devait analyser les banques de données

médicales (« *ensuring privacy protection while correlating widely differing data and sources* ») pour détecter la progression anormale de maladies pouvant être causées par des attaques biologiques. Il fut renommé « Bio-Alirt » (*Bio-event Advanced Leading Indicator Recognition Technology*) en janvier 2003 pour des fins de relations publiques.

— EELD (*Evidence Extraction and Link Discovery*). EELD visait à établir des liens entre des transactions informatiques variées à partir de sources publiques (par exemple, des sites internet) et de sources confidentielles (par exemple, des courriels) et à identifier les groupes et les individus liés à ces *patterns*. Le programme était sensé pouvoir induire les intentions des auteurs des transactions repérées et produire des scénarios d'actions plausibles. Le logiciel *Critical Intent Modeler* (CIM) utilisé par EELD provient à l'origine du projet Genoa I, réalisé en partenariat avec les firmes privées Veridian Corp., Groove Networks, Microsoft et Intel. Il s'agit d'un instrument qui tente d'extraire d'un ensemble de données partagées par plusieurs acteurs des hypothèses sur les décisions auxquelles ils parviendront. Appliqué à l'analyse des menaces terroristes, il permet de produire une série de scénarios accompagnés d'un compte-rendu complet du processus décisionnel suivi par les participants potentiels à un complot. L'illustration fournie à l'époque par l'IAO montrait l'établissement de liens de complicité entre les divers participants à une opération visant à voler de l'uranium enrichi (une organisation externe planifiant le vol, des complices à l'intérieur d'une entreprise, des intermédiaires à l'extérieur de l'entreprise — un fabriquant de cylindres pour le stockage de l'uranium, un transporteur et divers autres auxiliaires).

— *WAE* : *Wargaming the Asymmetric Environment*. La notion de conflit asymétrique fut développée par les militaires pour désigner une lutte armée au sein de laquelle s'affrontaient non pas deux entités de même nature (par exemple, deux États) mais deux belligérants de statut et, surtout, de force différents. Le terrorisme où s'affrontent un État et des organisations aux ramifications variables constitue le prototype du conflit asymétrique. Ce programme, semblable aux exercices théoriques auxquels se livrent tous les militaires (*kriegspiel*), transposait dans le contexte d'un conflit asymétrique les simulations habituellement effectuées par les états-majors des armées. Les objectifs et les méthodes sont à peu près les mêmes que dans le cas des simulations de conflits symétriques traditionnels.

— *Genoa II*. Le vice-amiral Poindexter, seul directeur de l'IAO durant la courte vie du département, avait été vice-président de l'entreprise *Syntek Technologies* et responsable du projet *Genoa* de cette firme, développé sous contrat avec la DARPA. Genoa visait à organiser les données recueillies selon leur importance et leurs interactions pour en rendre l'accès facile à plusieurs acteurs. Genoa II visait à rien de moins qu'à l'amélioration des processus cognitifs des analystes en réduisant la complexité des systèmes sans la dissoudre. Il s'agit d'une interface dynamique qui permettrait à tous les participants d'ajouter de l'information à différents paliers d'une conjoncture tout en conservant un modèle structuré et accessible à tous dans sa totalité. Le système inclut tous les documents nécessaires, toutes les notes des participants, un modèle structuré de la situation et permet l'échange immédiat d'idées, de solutions, de questions, et ainsi de suite.

— FutureMAP (*Futures Markets Applied to Prediction*). Ce programme se révéla

être un des plus solides clous dans le cercueil de l'IAO/TIA. La face publique de FururеMap était un site sur la toile où des investisseurs dûment enregistrés pouvaient engager des sommes selon leur évaluation de diverses situations politiquement explosives sur le globe. Les probabilités des issues possibles de ces situations servaient d'échelle de bénéfice pour les investisseurs. Bien que les créateurs du projet aient visé l'utilisation de la supposée puissance prédictive des marchés boursiers pour prévoir les situations dangereuses pour les intérêts étatsuniens, le tout fut présenté dans les médias comme un système de paris sur des assassinats de leaders internationaux, un désastre politique pour la DARPA. Le site fut retiré du serveur avant même son entrée en fonction.

D. *Évaluation*

Le trait le plus manifeste des instruments que nous avons brièvement présentés est leur caractère hétéroclite, sinon hétérogène. Ils appartiennent à quatre catégories : (1) Les outils d'identification : HumanID ; (2) la constitution de banques de données compréhensives : Genisys, Bio-surveillance ; (3) l'optimalisation des capacités d'analyse par la reconnaissance des *patterns* et par la prévision des décisions hostiles : EELD, Genoa II, WAE , FutureMap ; (4) les instruments de traduction informatisée : EARS, Babylon, TIDES.

Non seulement l'intégration de ces instruments en un système cohérent resta toujours douteuse, mais l'expérience que nous avons acquise nous autorise à être sceptiques à l'égard de certains de ces projets. L'Université de Montréal, à laquelle les deux auteurs de ce texte appartiennent, s'est longtemps spécialisée dans des programmes de traduction automatique. Son centre de recherche en la matière a cessé d'être subventionné quand, après des années de recherches infructueuses, il a même achoppé à traduire des bulletins de météo, dont on sait à quel point ils utilisent un vocabulaire répétitif et une syntaxe élémentaire. C'est pourquoi on peut douter de l'efficacité de programmes de traduction automatique qui ambitionnent de traduire des conversations entre terroristes, qui utilisent un langage allusif, fortement métaphorique, quand il n'est pas hermétiquement encrypté. On doit d'ailleurs s'étonner de l'absence de programmes de décryptage au sein de la TIA (Kippenhahn, 1999). Or, les programmes de traduction sont les seuls qui ont survécu au naufrage budgétaire.

Le second des traits évidents de l'IAO/TIA est son ambition, à certains égards vertigineuse. Le programme proposait une solution technologique aux lacunes identifiées par la commission conjointe de la Chambre des représentants et du Sénat dans les activités de la communauté du renseignement. Ces lacunes tiennent dans les conséquences de l'obligation légale de respecter la vie privée des citoyens des États-Unis, obligation en effet génératrice de dysfonctions imprévues, à savoir, le ciblage exclusif des étrangers, une culture du cloisonnement de l'information faisant obstacle à l'intégration horizontale du renseignement et une coupure entre le renseignement et son application, qui empêche la concertation verticales des acteurs de l'anti-terrorisme et qui dresse les uns contre les autres intervenants et analystes, policiers et agents de renseignement.

Voyons comment le programme TIA aurait dû permettre, en théorie, de résoudre

ces difficultés.

— *La protection de la vie privée*. C'était la partie la plus originale de la TIA et un de ses concepts fondateurs. On passera vite sur les instruments qui étaient sensés permettre la dé-nominalisation des informations, car là n'est pas l'essentiel. L'essentiel réside dans la volonté d'exercer, au moyen d'ordinateurs étroitement programmés, une surveillance informatique sur un flux de transactions *qui sont dissociées de leurs acteurs réels* à moins qu'ils ne suivent un *pattern* informatiquement normalisé (séquence d'étapes ou événement-clé) qui présente une menace. C'est en théorie dans ce seul cas que l'alerte aurait été déclenchée et que l'on serait passé du monitoring des *patterns* à la surveillance directe de leurs acteurs (et à leur appréhension éventuelle). Ce concept est en rupture avec l'exercice traditionnel de la surveillance, où elle est une démarche *inductive* qui rattache des comportements individuels à une menace ou un risque général (collectif) souvent imparfaitement conceptualisés. Des individus en surveillent d'autres et infèrent progressivement que leur comportement menace une entité abstraite (l'État, la collectivité, le clan et ainsi de suite). Par contraste, la TIA tenait davantage de la nature d'une *déduction*, c'est-à-dire quelle procédait du général — des *patterns* types reconstitués par l'analyse — au particulier (les acteurs réels). À n'en pas douter, les transactions dont le flux quotidien est examiné par la machine étaient individuelles, mais elles n'étaient pas encore *individuées*. La surveillance des transactions se serait produite sous le voile de l'ignorance des opérateurs du système pour ce qui est de l'identification des parties à ces transactions. Le processus d'identification ne devait être déclenché qu'à partir du repérage d'un *pattern* menaçant et suivait une démarche quasi-syllogistique dont voici les prémisses :

prémisse universelle	Tous les initiateurs du *pattern* A sont dangereux
énoncé particulier	Quelque (au moins un) X est un train d'enclencher ce *pattern*
inférence	Cet X est dangereux
stade d'identification	Qui est X ? (Déclenchement de l'alerte)
identification réelle	X=A (a)……. A (n)
prémisse normative	il faut arrêter les gens dangereux
conclusion pratique	A(a) est recherché/arrêté

Ce schéma est évidemment simplifié. Nous reviendrons en conclusion sur sa signification.

— *Désuétude des règles de ciblage exclusif des étrangers.* Cette exclusivité, on l'a vu, provient en grande partie d'une réponse apportée par le pouvoir aux inquiétudes des citoyens des États-Unis sur la protection de leur vie privée. Comme la TIA offrait une solution indépendante à ce problème, il aurait été inutile de continuer à recourir à la solution antérieure, à la fois désuète et disfonctionnelle. Donc, la TIA pouvait (en fait,

elle *devait*) cibler autant les autochtones que les étrangers.

— *L'intégration horizontale*. Nous avons tenté de montrer que la culture du cloisonnement de l'information s'était progressivement développée à partir des limitations apposées au ciblage des sujets du renseignement, les services s'étant vus assigner leur clientèle spécifique : les services de sécurité s'occupent des étrangers et la police des autochtones. Les limitations du ciblage étant levées, l'intégration horizontale serait libérée d'un obstacle majeur à son développement. En fait, la TIA aurait pu donner lieur à une intégration horizontale du renseignement d'une multitude de façons, car la mise en réseau de toutes les sources de données et le croisement tous azimuts de l'information était sa raison d'être originelle. Nous avons au passage souligné les efforts explicites du programme en ce sens.

— *La concertation verticale*. Le manque d'intégration verticale a pris trois formes : fracture entre la cueillette et l'utilisation du renseignement, coupure entre le renseignement de terrain et son analyse et divorce entre les services de renseignement et la police. Notre description des instruments mobilisés par la TIA montre à quel point le développement de l'analyse et de l'exploitation du renseignement constitue une des priorités du programme. Or, les outils d'analyse (Genisys, Genoa II, EELD) étaient centrés sur la prévision du passage à l'acte de terroristes. La contrepartie de cette focalisation était un accent nouveau placé sur la prévention efficace de ce passage à l'acte par le développement de politiques d'intervention et par l'instrumentalisation des intervenants eux-mêmes. Ces intervenants étant, pour la majorité d'entre eux, des policiers, la TIA aurait par conséquent intégré leur action. Il faut toutefois reconnaître que la TIA ne prévoyait pas encore de solution explicite à la coordination entre les services de renseignement et la police, qu'elle appelait de ses vœux sans proposer les moyens de la réaliser. Il faut à cet égard se souvenir que l'IAO/TIA était sous l'égide du ministère de la Défense, dont les préoccupations sont relativement éloignées de celles de la police.

E. *La descendance de la TIA*

Sous les attaques répétées des défenseurs du droit à la vie privée, le Congrès interdit en février 2003 que la TIA vise les citoyens étatsuniens. Ce fut pour les concepteurs et les avocats du programme un important recul. Néanmoins, les attaques ne diminuèrent pas, et après le scandale du FutureMap le Sénat coupa entièrement les vivres à la DARPA en ce qui concerne l'IAO et la plupart des sous-projets liés à la TIA.

La mort du projet TIA, loin de décourager le développement de technologies d'exploration de données, semble avoir multiplié les efforts en ce sens en décentralisant les projets existants. Les firmes ayant travaillé sous contrat avec l'IAO, privées de leurs sources de revenus lors de sa disparition, ont offert leurs services ailleurs. Les têtes dirigeantes de l'IAO ont trouvé d'autres endroits où mettre leur expertise à profit — par exemple, une sous-directrice responsable de l'IAO à la DARPA, Jane Alexander, est maintenant responsable de projets à l'HSARPA, l'équivalent de la DARPA au Department of Homeland Security. Sa première réalisation est le système CAPPS II, que la Transportation Security Administration (TSA) utilisera bientôt pour filtrer les passagers de lignes aériennes en vérifiant certaines de leurs activités passées auprès

de multiples banques de données privées et publiques. L'Advanced Research and Development Activity (ARDA), une agence de l'Intelligence Community et du Department of Defense, développe activement des technologies avec l'aide des anciens partenaires privées de l'IAO. La DARPA n'est pas en reste avec son nouveau programme « LifeLog », ou « journal de vie », qui vise entre autres à permettre la filature électronique de personnes à partir des traces informatiques qu'elles laissent et qui sont reconnaissables comme autant de patterns personnels. En principe rien ne s'oppose à ce que LifeLog puisse suivre les traces de millions de personnes à la fois, au quotidien. Dernier exemple, le système MATRIX, ou « Multistate Anti-Terrorism Information eXchange », déjà en fonction dans plusieurs États, met en commun la plupart des banques de données gouvernementales (permis de conduire, dossier criminel, enregistrement de véhicules, etc.) pour identifier des pistes d'enquête.

La création de programmes apparentés à la TIA n'est pas la seule mesure de l'administration du président Bush pour remédier aux déficiences alléguées de la surveillance politique aux Etats-Unis. La législation la plus compréhensive à cet égard demeure le USA Patriot Act qui, tout comme la Loi antiterroriste canadienne, fut voté dans les mois suivant les attentats de septembre 2001. La section 218 du Patriot Act remédie à ce qui a été dénoncé comme une interprétation erronée de la loi FISA, à savoir, qu'elle autorisait exclusivement des opérations de surveillance politique et de cueillette de renseignements contre les étrangers et qu'elle était préjudiciable à la coordination entre la police et les services de renseignement. Cette section stipule qu'on pourra opérer contre les étrangers dans tout « but significatif » et non seulement pour des fins de renseignement. En rapprochant le renseignement et l'intervention, de même que les services de sécurité et la police, le Patriot Act affaiblit la frontière entre la surveillance des étrangers et celle des Étasuniens « en titre » : le rapprochement entre les agences entraîne la plupart du temps celui de leur clientèle respective.

3. *CONCLUSIONS : LA NOUVELLE SURVEILLANCE*

Il est évidemment prématuré de penser qu'un nouveau paradigme de la surveillance est en train de se mettre en place, quelque trois ans après les attentats de septembre 2001. Aussi, est-ce à titre d'hypothèses que nous soumettons un ensemble de caractéristiques qui nous semblent propres au dispositif qui commence à s'instituer en Amérique du Nord. Cette caractérisation est à beaucoup d'égards l'aboutissement de tendances qui s'étaient manifestées bien avant le 11 septembre 2001.

A. *Le primat de la technologie : SIGINT vs HUMINT*

La première conclusion qui suit de nos observations est la croissance exponentielle de la surveillance exercée par le moyen de la technologie. On peut la constater tant au Canada qu'aux Etats-Unis. Au Canada, des agences comme le CST jouent maintenant, bien que de façon discrète, un rôle de premier plan, comme la NSA aux Etats-Unis. Ce développement est ancien. La création de l'IAO et le développement de la TIA furent toutefois des innovations qui soulignent l'arrivée d'une technologie particulière dans le champ de la surveillance, à savoir, l'informatique. Un nombre important des firmes sous

contrat avec la DARPA sont des entreprises en informatique (Syntek Technologies, Booz, Allen Hamilton Inc., Hicks and Associates, Microsoft, Intel et Veridian Corporation, pour n'en nommer que quelques-unes).

Outre l'air du temps, le recours croissant à la technologie s'explique par deux facteurs. Le premier est la difficulté de plus en plus considérable d'infiltrer les groupes terroristes (comme, d'ailleurs, ceux du crime organisé ; voir United States, 1996), qui marque un recul notable de l'HUMINT. Un grand nombre de ces groupes ayant été formés sur d'autres continents que l'Amérique du Nord ou l'Europe, il est difficile pour un agent d'un service nord-américain ou européen de se faire passer pour un candidat potentiel au recrutement dans un de ces groupes (différences de langue, d'apparence physique et ainsi de suite). En outre, pour se protéger contre l'infiltration, plusieurs de ces groupes exigent la commission d'un crime grave (un assassinat) pour admettre un membre. Or, il est interdit aux agents des services de renseignement de commettre ce genre de crime, serait-ce pour assurer leur couverture (Brodeur, 1992). Le second facteur tient dans la critique sévère qui est faite des aptitudes de la police, trop obsédée par l'élucidation d'affaires particulières, au travail de renseignement. « *Les analystes du renseignement feraient sans doute de mauvais policiers, comme il est devenu très clair que les policiers sont de mauvais analystes du renseignement* » (Shelby, 2002 : 62). Cette critique du sénateur Shelby est dirigée contre l'élite de la police étatsunienne, à savoir, le FBI. Elle s'applique d'autant plus aux forces policières dont les capacités d'enquête sont inférieures à celle du FBI.

B. *L'adversaire et l'ennemi*

La critique de la police, aussi sévère soit-elle, ne signifie pas qu'on l'abandonne à son sort. On tente de la réformer, mais plusieurs de ces réformes procèdent de l'extérieur. Au Canada, par exemple, nous avons vu que le mandat du CST avait été élargi pour que le Centre prête assistance à la police. Aux États-Unis, de multiples technologies informatiques visent à réduire l'écart entre le renseignement et son utilisation dans l'application des lois pénales, les policiers ayant été explicitement désignés comme des destinataires des banques de données créées par la TIA, par exemple. Il faut toutefois signaler que tant le CST, au Canada, que l'IAO/TIA, aux Etats-Unis, sont des créations de ministères de la défense et de hiérarchies militaires. Le rapprochement entre la police et l'armée par culte interposé du renseignement pourrait avoir pour conséquence un changement de paradigme dans la définition des cibles de la police, davantage conçues comme des *ennemis* à neutraliser que comme des *adversaires* de l'intérieur dont la réinsertion sociale est concevable. Cette pénétration des représentations et des mœurs de l'armée au sein de la police — pensons simplement aux répercussions du mot d'ordre emblématique de faire la « guerre au terrorisme », qui a amené une redéfinition des policiers comme « combattants » (*warfighters*) — est susceptible d'altérer la distinction entre sécurité intérieure et sécurité extérieure.

C*. Surveillance inductive et surveillance déductive*

Nous avons déjà esquissé un type relativement nouveau de démarche de surveillance, qui mobilise un arsenal de *patterns* types — séquences risques, événements clés et

ainsi de suite — pour ensuite procéder à l'identification d'infracteurs réels ou potentiels. Nous avons également souligné que cette démarche, que nous avons extraite de notre analyse du programme TIA, ne lui est pas limitée et constitue une tendance véritable. La manifestation la plus répandue de cette tendance tient dans les diverses formes du profilage au sein de la police. Le profilage constitue dans certains cas une pratique officielle et valorisée (bien qu'embryonnaire), comme dans le cas des enquêtes sur des tueurs en série et, de façon plus générale, dans la répression de la délinquance sexuelle violente. Il constitue également un procédé officieux, reprouvé sous l'appellation de délit de faciès ou de profilage ethnique.

Les surveillants se sont toujours avancés vers leurs cibles à partir de leurs préconceptions et de leurs préjugés. Ce qui est innovateur dans la surveillance déductive, c'est un effort délibéré et scientifiquement instrumenté pour remplacer ces préventions arbitraires incrustées dans la pratique par des modèles objectivés qu'un apport nouveau d'information peut en théorie modifier. Sans préjuger du succès de cet effort — peut-être l'empirisme est-il « l'horizon indépassable » de la surveillance — on peut faire l'hypothèse qu'il pourrait cliver la surveillance. On aurait d'une part les effectifs déployés sur le terrain qui fonctionnent à l'induction et au coup par coup, dans le meilleur des cas, et qui marchent au stéréotype et à la rafle, dans le pire. D'autre part, se constituerait un corps de surveillants à distance scrutant le terrain au travers de modèles du risque intégrés au programme de leurs machines et qui instrumentalisent au besoin les effectifs de terrain pour effectuer des frappes d'ampleur variable (voir par exemple Leman-Langlois, 2003).

D. *Privatisation de la surveillance*

Toute pénétration de la technologie s'accompagne d'un recours concomitant au secteur privé, qui est le grand pourvoyeur de technologie. La grande erreur en ce domaine est de croire que l'utilisateur est le maître de son instrument. Cette croyance est doublement fausse.

Il faut en première part distinguer entre l'opération individuelle et l'effet de système. On ne saurait nier qu'un policier peut piloter son véhicule automobile là où il veut aller. On ne saurait davantage nier que l'irruption de l'automobile a transformé la police de façon non prévue en mettant entre elle et la population la distance de ses véhicules. On ne peut encore apprécier les effets systémiques de la technologie de surveillance, mais on peut s'attendre à ce qu'ils transforment les pratiques d'une façon que nous n'avions pas anticipée. Pour prendre un exemple simple, Ericson et Haggerty (1997) ont bien montré que l'introduction de l'ordinateur dans les voitures de patrouille de la police était une arme à deux tranchants. Elle augmente la capacité de surveillance des patrouilleurs en leur permettant d'effectuant tout un ensemble de contrôles informatiques — en particulier, à partir des plaques d'immatriculation des véhicules qu'ils surveillent. D'autre part, elle rend ces patrouilleurs beaucoup plus vulnérables à leur propre surveillance par la hiérarchie puisque toute utilisation de l'ordinateur laisse des traces repérables et comptabilisables et qu'on peut savoir de façon beaucoup plus précise « ce que fait la police » (Monjardet, 1995) depuis qu'elle utilise des ordinateurs.

On doit en seconde part insister sur une donne capitale de l'utilisation de la

technologie. A l'origine, un nouvel instrument technologique est la plupart du temps taillé sur mesure pour répondre à un besoin particulier. Cependant, quand une technologie obtient un succès initial important et qu'elle est reproduite à grande échelle, elle ne correspond plus de façon exacte aux besoins précis de ceux l'importent. En généralisant cet exemple, on parvient à la proposition suivante : *l'acquisition d'instruments technologiques n'est pas dans la majorité des cas gouvernée par un principe d'adéquation mais par un principe de disponibilité*. En d'autres termes, celui qui investit dans la technologie ne se procure pas tant l'instrument adéquat que l'instrument disponible, la distance entre les deux variant de manière considérable. C'est du fond de ce creux entre l'adéquat et le disponible que proviennent les effets non anticipé de l'adoption d'une technologie par une profession.

E. *Les risques d'erreurs*

Toute inscription peut comporter une erreur (nom mal orthographié, numéro mal donné ou mal saisi et ainsi de suite). Quand on les effectue, les vérifications de la validité des informations contenues dans les banques de données de la police et (plus rarement) des services de renseignement révèlent un pourcentage très élevé d'erreur (des audits effectués par les vérificateurs étatsuniens ou canadiens ont relevé des erreurs plus ou moins significatives dans 40% des inscriptions).

La multiplication des banques de données et la recherche de *patterns* est doublement vulnérable à l'erreur. Un ensemble d'erreurs peut se d'abord se glisser dans la saisie des données. À ce premier type d'erreur, s'ajouteront ensuite les erreurs d'analyse qui seront d'au moins deux sortes. En première part, les analyses fondées sur des données corrompues délibérément ou par accident seront par définition sans validité. En deuxième part, lorsque les données seront sûres, le risque d'erreur de l'analyste (personne humaine ou logiciel mal conçu) ne peut jamais être écarté. En dépit du début d'engouement dont ils bénéficient, on sait que les profils bricolés pour identifier des tueurs en série ont été d'un piètre apport pour les enquêteurs et les ont parfois amenés sur de fausses pistes. Rien ne nous assure que les *patterns* caractéristiques de l'action terroriste seront véritablement discriminants. On peut s'acheter un billet d'avion en payant en espèces et en laissant la date du retour indéterminée pour un ensemble considérable de raisons qui n'ont rien à voir avec le terrorisme.

F. « *L'exubérance irrationnelle* »

Cette expression a été forgée par M. Allan Greenspan, le président de la banque centrale des Etats-Unis, pour désigner l'euphorie spéculative sur les marchés boursiers, lors du gonflement de la « bulle » générée par la nouvelle économie de l'information. On sait ce qu'il en advint par la suite.

Il y a certains indices à l'effet que le même type d'exubérance s'est emparé d'une partie de la communauté du renseignement aux Etats-Unis. Par exemple, le logo de l'IAO était une pyramide dont la pointe enchâsse un gros œil irradiant des rayons solaires, qui observe en surplomb la planète Terre. Au bas du logo est gravée la devise de l'IAO en bas latin : « Scientia est Potentia ». Cette triomphante cuistrerie, qu'on fit

rapidement disparaître du site internet de l'IAO au début de la controverse, rappelle à s'y méprendre l'optimisme des loges maçonniques célébrées par Mozart dans *La flûte enchantée* (le logo original peut être vu ici : http://www.mapageweb.umontreal.ca/brodeuj/tia.htm). De façon plus significative, on comprend mal que l'IAO s'avance sans masque dans le champ miné de la traduction automatique, dont la plupart des linguistes ont désespéré. Espère-t-on que des programmes informatisés qui ont échoué à traduire des bulletins de météorologie divulgueront en bon anglais la stratégie d'Al Quaida ou celle de l'Axe du mal? L'une des déficiences reconnues de la communauté du renseignement aux Etats-Unis est le manque de compétence dans la compréhension des communications en langue étrangère. Il n'est suit pas qu'il faille s'en remettre les mains jointes à l'ordinateur pour remédier à cette difficulté, comme si tout ce qui en sortait avait le prestige d'une appellation d'origine contrôlée.

Il faut évidemment souhaiter que la réforme de la communauté du renseignement dépasse cette phase d'exubérance avant qu'elle ne génère une bulle qui finira à brève échéance par éclater, emportant avec elle une masse de spéculateurs. Il faudra toutefois s'interroger si le côté occulte du renseignement ne secrète pas une mythomanie qui persiste parce qu'on est empêché de la révéler dans sa vérité. Un lieutenant de police du XVIII^{e} siècle — M. de Sartine — assura au roi qu'il se trouvait un indicateur à lui dans chaque rassemblement de trois personnes. Cela n'a pas empêché que la Révolution n'éclatât avant la fin du siècle.

G. *Une surveillance planétaire*

Les instruments de la surveillance totale que nous avons décrits sont pour l'essentiel constitués par une technologie initialement créée par le CST et la NSA, qui sont des agences militaires de surveillance et dont la vocation est d'emblée planétaire, comme l'a révélé le programme ECHELON, qui inquiète légitimement les Européens. En outre, les cibles de la nouvelle surveillance sont d'abord désignées comme des « étrangers », afin de rassurer les citoyens inquiets d'un état et leurs représentants. Il faut d'abord remarquer, à cet égard, que la catégorie d'étranger est globalisante : si l'on fait le total de tous ceux qui sont considérés étrangers par les divers pays de la planète pris un à un, on engendre ainsi la population mondiale. Mais, de façon plus profonde, l'évolution du CST et de la surveillance politique aux Etats-Unis, enseigne que c'est moins l'étranger qui est la cible que ce que nous appellerons « l'individu en réseau ». L'étendue des réseaux au sein desquels nous sommes tous à divers degrés insérés nous projette constamment hors de nous-mêmes et fait de nous des étrangers potentiels au regard des appareils de surveillance. C'était déjà là tout le mécanisme des procès staliniens, où il suffisait de démontrer qu'un accusé avait un lien quelconque avec l'étranger pour obtenir sa condamnation.

Les termes de « mondialisation » et de « globalisation » apparaissent comme les nouveaux sésames de la pensée. Les pages qui précèdent montrent qu'il y a une grande part d'effervescence vite retombée dans tous ces desseins de surveillance planétaire : si la coopération internationale entre les forces de police et les services de sécurité est aussi brouillonne que les relations tortueuses établies entre les services

d'un même pays, comme les États-Unis, la terreur peut dormir tranquille. La terreur, peut-être, mais pas nous. Nous sommes entrés dans une période de transition qu'on pourrait baptiser de l'appellation « surveillance-fiction », tant à cause de ses ambitions démesurées que par la cacophonie des moyens hétéroclites mobilisés pour les réaliser. On pourrait cependant faire valoir que la surveillance-fiction est encore plus dangereuse que la surveillance efficace pour les libertés civiles, à cause de son potentiel illimité de générer des erreurs de surveillance.

Sources citées

Brodeur, Jean-Paul, Gill Peter and Töllborg Dennis (2003), *Democracy, Law and Security. Internal Services in Contemporary Europe*, Aldershot: Ashgate.

Brodeur, Jean-Paul (2003), "The Globalization of Security and Intelligence Agencies: a Report on the Canadian Intelligence Community" in Brodeur, Jean-Paul, Peter Gill and Dennis Töllborg (2003), *Democracy, Law and Security. Internal Services in Contemporary Europe*, Aldershot: Ashgate, p. 210-261.

Brodeur, Jean-Paul (2000), "Cops and spooks", *Police Practice and Research*, Vol. 1, No. 3, p. 299-321

Brodeur, Jean-Paul (1992), "Undercover policing in Canada: Wanting what is wrong", *Crime, Law and Social Change*, No. 18, p. 105-136

Ericson, Richard V. and Kevin Haggerty (1997), *Policing the Risk Society*, Toronto and Buffalo: University of Toronto Press.

Kippenhahn, Rudolf (1999), *Code Breaking. A History and Exploration*. New York: The Overlook Press.

Leman-Langlois, Stéphane (2003), « The Myopic Panopticon: the Social Consequences of Policing Through the Lens », *Policing and Society*, 13 (1), 43-58.

Monjardet, Dominique (1996), *Ce que fait la police*, Paris : La découverte.

Nislow, Jennifer (2002), « A very special agent », *Law Enforcement News*, Vol. 28, No. 589-590, December 15/31 2002, 1-3 (ce dossier reproduit des extraits de la lettre très critique des agissements du FBI que l'agent Rowley fit parvenir au directeur de ce service, M. Robert Mueller).

Plenel, Edwy (1997), *Les mots volés*, Paris : Stock.

Québec (1981), *Rapport de la Commission d'enquête sur des opérations policières en*

territoire québécois, Québec : ministère de la Justice.

Shelby, Richard C. (2002), *September 11 and the Imperative of Reform in the U.S. Intelligence Community. Additional views of Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence*, United States Senate Select Committee on Intelligence, Washington D.C. : US Government Printing Office. On peut trouver cette publication sur l'Internet http://intelligence.senate.gov/pubs107.htm

United States, Congress, Senate, Select Committee to Study Governmental Operations With
Respect to Intelligence Activities, 94th Congress, 2nd Session (1976), *Intelligence Activities*
and the Rights of Americans (The Church Report), Washington (D.C.), US Government Printing Office.

United States, Congress, House, Select Committee on Intelligence (1977), *CIA : The Pike Report,* Nottingham, Spokesman Books for the Bertrand Russel Peace Foundation

United States, Congress (1996), *Preparing for the 21st Century. An Appraisal of U.S. Intelligence*, Report of the US Congress Commission on the Review of American Intelligence (Harold Brown, Chairman). Washington, D.C. : US Government Printing Office. On peut trouver cette publication sur l'Internet:
www.access.gpo.gov/int/int002.html

United States, Congress (2002), *Joint Inquiry conducted by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Findings and Recommendations*, Washington D.C.: US Government Printing Office. On peut trouver cette publication sur l'Internet http://intelligence.senate.gov/pubs107.htm

Sources internet

Pages mises à jour
a) http://erta-tcrg.org/tia.htm
b) http://erta-tcrg.org/datamining.htm

1. EPIC (Electronic Privacy Information Center) :
http://www.epic.org/privacy/profiling/tia/
2. FERET et Face Recognition Vendor Test : http://www.frvt.org/
3. Government exec.com : http://www.govexec.com/dailyfed/1102/112002ti.htm
4. IAO : http://www.darpa.mil/iao/index.htm
5. New Tools for Domestic Spying, and Qualms (*Cryptome*) http://cryptome.org/tia-balk.htm
6. New York Times : http://www.nytimes.com/2002/11/09/politics/09COMP.html

7. Total Information Awareness Program (TIA) System Description Document (SDD) (document officiel, 150 pp.):
http://www.epic.org/privacy/profiling/tia/tiasystemdescription.pdf
8. Washington Post : http://www.washingtonpost.com/ac2/wp-dyn/A40942-2002Nov11