Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 24 (2006)

Artikel: Les nouvelles technologies font-elles baisser la criminalité?

Autor: Cusson, Maurice

DOI: https://doi.org/10.5169/seals-1051073

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 20.11.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

MAURICE CUSSON

LES NOUVELLES TECHNOLOGIES FONT-ELLES BAISSER LA CRIMINALITÉ?

Resumé
Les nouvelles technologies pourraient aussi bien faire reculer la criminalité que la faire augmenter. En revanche, il serait possible que les technologies de la sécurité préviennent la criminalité dans les sites où elles sont correctement mises en place. Les technologies examinées sont:
1 la télésurveillance
2 les contrôles d'accès
3 les systèmes d'alarme.
L'installation de techniques de sécurité dans une organisation offre de bonnes chances de faire reculer la criminalité, mais un effet durable ne peut être maintenu que si le personnel de sécurité reste vigilant et disposé à intervenir. Les programmes de prévention comportant plusieurs volets intégrés les uns aux autres obtiennent de meilleurs résultats que ceux qui n'utilisent qu'une seule mesure. En effet, un éventail intégré de mesures variées permet à l'action de sécurité d'atteindre un niveau d'intensité suffisant, assure l'étanchéité de la protection et permet une meilleure adaptation des réponses aux problèmes.

Drängen die neuen Technologien die Kriminalität zurück?
Die neuen Technologien können die Kriminalität genau so gut steigern wie mindern. Möglich ist indes auch, dass die Sicherheitstechnologien Kriminalität dort verhindern, wo sie korrekt gebraucht werden. Die analysierten Technologien sind:
1. Videoüberwachung
2. Zugangskontrollen und
3. Alarmsysteme.
Die Verwendung von Sicherheitstechnologien innerhalb einer Organisation bietet gute Chancen, die Kriminalität zu senken, aber eine dauerhafte Wirkung kann nur erreicht werden, wenn das Sicherheitspersonal wachsam bleibt und zur Intervention bereit ist. Präventionsprogramme, die verschiedene integrierte Massnahmen enthalten die aufeinander abgestimmt sind, erreichen bessere Resultate als diejenigen, die nur eine Massnahme enthalten. Die Integration unterschiedlicher Massnahmen ermöglicht, ein ausreichendes Sicherheitsniveau zu erreichen, stellt sicher, dass Lücken geschlossen werden können und erlaubt eine bessere Anpassung der Massnahmen an die Problemlage.

Au début de ma réflexion sur le thème de votre congrès, j'inclinais à penser que les nouvelles technologies ont bien tendance à faire baisser la criminalité. Puis j'ai trouvé quatre raisons pour lesquelles cette évolution technologique réduit la criminalité et quatre raisons de penser qu'elles la font monter.

1. Les progrès technologiques permettent aux manufacturiers de concevoir et de fabriquer de plus en plus de produits à l'épreuve du vol. Cela vaut pour les véhicules automobiles, les radios, les télévisions, les ordinateurs et bien d'autres produits. Il est possible en effet d'incorporer dans ces appareils des anti-vols, des alarme et des puces qui aident à l'identification en cas de vol et qui permettent de retracer un produit, notamment en utilisant le G.P.S.
2. L'utilisation massive des cartes de crédit et des cartes guichet limite la circulation de l'argent liquide cependant que la technologie permet de sécuriser ces cartes (FELSON 1998).
3. Les longues heures passées à surfer sur Internet, à jouer à des jeux vidéo, à regarder la télévision et le cinéma maison ne peuvent pas être consacrées à circuler dans les rues, dans les magasins, dans les bars et dans les autres lieux où on tombe sur des occasions de commettre des délits et d'en être victime. (Cette idée est de MARC OUIMET). Les nouvelles technologies sédentarisent les gens et les protègent contre la délinquance et la victimisation.
4. Les nouvelles technologies de la sécurité comme la vidéosurveillance et les systèmes de contrôle d'accès se sont généralisées tout en devenant de plus en plus performantes. Leur capacité de prévenir le crime est considérable. J'y reviendrai.

Inversement, les raisons de penser que les nouvelles technologies poussent la criminalité à la hausse sont aussi nombreuses et convaincantes. J'en vois quatre:

1. Le développement technologique se traduit par la mise sur le marché de produits tentants et faciles à voler, comme les disques compacts, les téléphones et ordinateurs portables, les baladeurs, etc.
2. De nouveaux outils et appareils peuvent être détournés de leurs fins et utilisés par les voleurs et les fraudeurs. Par exemple, les

perceuses électriques sans fil sont bien utiles pour les cambrioleurs et les imprimantes couleur aident les fraudeurs à fabriquer de faux billets ou de faux documents.

3. Grâce à l'Internet, les fraudeurs développent de nouveaux moyens d'escroquer les gens et ils ont accès facilement et rapidement à d'immenses quantités de victimes potentielles.
4. Il n'est pas inutile de rappeler le passé récent. Entre 1960 et 1980, la criminalité a augmenté fortement dans la plupart des démocraties occidentales. – sauf en Suisse. Or, durant la même époque, on enregistrait dans ces pays une forte croissance de l'économie et de la technologie.

En somme, l'évolution technologique souffle le chaud et le froid, produisant des effets opposés qui s'annulent mutuellement.

À la réflexion, la question posée dans le titre de cette communication est située à niveau d'agrégation si élevée que l'hypothèse devient infalsifiable. D'autant plus que la criminalité d'un pays fluctue dans un système ouvert à l'influence de toutes sortes d'autres facteurs, comme la structure familiale, la composition démographique, la consommation de drogues et d'alcool, les inégalités sociales, les contrôles sociaux … Pour me sortir de cette impasse, j'ai décidé de circonscrire le problème sans pour autant renoncer à l'hypothèse que les technologies font baisser la criminalité. La nouvelle question à laquelle je me propose donc de répondre s'énonce comme suit.

Est-il possible que les nouvelles technologies de la sécurité préviennent la criminalité dans les sites où elles sont correctement mises en place?

Cette question m'est venue à l'esprit en constatant qu'au Québec la plupart des grandes organisations privées, publiques ou parapubliques disposent d'un service interne de sécurité utilisant la télésurveillance, les systèmes de contrôle d'accès et d'autres technologies. Nous retrouvons ces équipements dans les banques, les commerces,

les industries, les sociétés de transport, les entrepôts, les hôpitaux, les stades... Si nous acceptons l'hypothèse optimiste voulant que les directeurs de la sécurité de ces organisations utilisent intelligemment les nouvelles technologies de la prévention, ils devraient réussir à sécuriser les sites dont ils sont responsables.

Une question posée en ces termes limite le propos de deux manières. Premièrement, je m'en tiens à la prévention, ce qui me dispense d'aborder le vaste domaine de la criminalistique et des technologies d'enquête, sujet sur lequel OLIVIER RIBAUX est infiniment plus compétent que je ne le suis. Deuxièmement, je m'enferme volontairement dans le «site» d'une organisation, c'est-à-dire à l'intérieur de ses terrains et bâtiments. Très souvent, il est possible pour une organisation de sécuriser ses sites et ses véhicules (dans le cas des sociétés de transport). Dans ces conditions, il est raisonnable de penser qu'un service de sécurité dispose des moyens humains et techniques suffisants pour contrôler la criminalité qui menace son organisation.

La réponse à la question ainsi reformulée tient en trois parties:

- Premièrement, je commencerai par présenter les trois principales technologies de prévention utilisées par les grandes organisations en insistant sur leur potentiel préventif.
- Deuxièmement, je discuterai de la place que ces technologies occupent dans les stratégies interdépendantes des chefs de la sécurité et des délinquants. J'y présenterai un concept dynamique de la prévention dans lequel les délinquants s'adaptent en permanence aux technologies mises en place pour les arrêter alors que les responsables de la sécurité s'adaptent à cette adaptation.
- Troisièmement, nous verrons comment les technologies de la prévention peuvent être coordonnées et mises en synergie pour produire de la sécurité au sein d'une organisation et faire reculer la criminalité.

1 Les technologies de la prévention

Les technologies préventives sur lesquelles je m'attarderai ne sont pas très nouvelles mais elles sont couramment utilisées et potentiellement efficaces. Il s'agit de la télésurveillance, des contrôles d'accès et des systèmes de détection et d'alarme.

La télésurveillance

La télésurveillance, le terme le dit, permet de voir loin, de voir ce qui se passe dans plusieurs lieux différents et d'enregistrer automatiquement les incidents et les anomalies. Quand de nombreuses caméras de surveillance sont installées dans divers endroits, un seul surveillant posté dans une centrale peut voir autant que quelques dizaines de gardes qui n'auraient que leurs yeux pour voir.

Des caméras visibles ont pour premier but de faire reculer des individus tentés de violer la loi. Elle produit donc un effet de *dissuasion situationnelle.* La deuxième fonction est de *guider une intervention* rapide sur les lieux d'un incident. Constatant une intrusion, une agression ou tout autre anomalie, le préposé d'une centrale de surveillance communique avec une personne placée à proximité et lui demande d'accourir. Le troisième but de la surveillance est *répressif.* Elle permet d'enregistrer les incidents et de confondre un coupable. Dans de tels cas, on utilise assez souvent des caméras cachées.

Un système de télésurveillance est formé de 3 éléments:

- Premièrement, des caméras (visibles ou invisibles; équipées ou non de zoom et de téléobjectif; pouvant ou non à être contrôlées à distance et être déclenchées par un mouvement inhabituel; pouvant ou non suivre automatiquement un individu dans ses déplacements).
- Deuxièmement, des moyens de retransmission de l'image captée par la caméra vers un moniteur.

- Troisièmement, une centrale de surveillance munie de moniteurs, magnétoscopes, voyants et autres avertisseurs.

Un système de télésurveillance peut être combiné à des détecteurs de mouvement, à un système d'alarme, à un appareil qui localise les sons et même à un appareil à rayons X pouvant détecter des armes dissimulées sous des vêtements (LEMAN-LANGLOIS et BRODEUR 2005).

Les contrôles d'accès

Ils ont trois fonctions:

1. *Filtrer* les personnes qui veulent entrer ou sortir d'un lieu ou encore les objets que l'on voudrait, soit introduire, soit faire sortir. Un système de contrôle d'accès laisse entrer les gens autorisés et interdit l'accès aux autres (suspects, bagarreurs connus, intrus, hooligans ...). Il peut aussi empêcher que l'on entre dans un établissement avec des armes ou des explosifs.
2. *Couper la fuite* des individus qui auraient commis un délit dans un lieu fermé. Un dispositif pour empêcher les gens d'entrer peut aussi être utilisé pour les empêcher de sortir. Il est possible, dans les banques, de bloquer la fuite d'un braqueur en l'enfermant entre deux portes fonctionnant comme un sas. Dans un magasin, les voleurs à l'étalage sont interceptés par des systèmes de détection des étiquettes électroniques ou magnétiques dissimulées dans les produits mis en vente.
3. *Diriger l'enquête.* Quand un dispositif de contrôle d'accès par carte s'accompagne d'un enregistrement des entrées et des sorties, on peut savoir qui se trouvait à l'endroit et au moment où un crime a été commis. C'est la fonction répressive des contrôles d'accès.

Bref, les contrôles d'entrée et de sortie rendent les crimes et les délits plus difficiles et plus risqués en empêchant les malfaiteurs d'a-

voir accès à leurs cibles, en les désarmant, en les empêchant de fuir et en facilitant les enquêtes.

Il est utile de distinguer deux éléments dans un système de contrôle d'accès:

1. *L'identification* permet de discriminer entre les individus qui sont autorisés à entrer ou à sortir et les autres. L'identification est directe et personnelle quand le préposé à l'entrée connaît bien les gens qui fréquentent l'établissement. Elle peut se faire par la présentation de la carte d'identité ou d'un passeport. Ensuite viennent les technologies de plus en plus sophistiquées: les clés, les codes entrés sur un clavier, les cartes magnétiques, les cartes à code barre, les cartes munies de circuits intégrés dont la mémoire contient des informations sur le porteur, les cartes de proximité contenant un émetteur passif (transpondeur) qu'un capteur peut lire à distance (le transpondeur réfléchit le signal émis par un émetteur-récepteur qui reconnaît la fréquence radio et identifie le porteur de la carte: WALSH 1995; LEMAN-LANGLOIS et BRODEUR 2005).
   Comme les cartes dont il vient d'être question peuvent être volées, perdues, prêtées, falsifiées ou copiées, on peut avoir recours à la *biométrie*. L'identification, dans ce cas, repose sur les particularités physiques propres d'une personne: ses empreintes digitales, la géométrie de sa main, son iris, sa rétine, sa voix, son visage. Un appareil «lit» l'empreinte des doigts, l'iris, etc. et en numérise la configuration. Ensuite un ordinateur équipé d'un logiciel approprié compare l'empreinte de l'individu avec celles qui ont été accumulées dans une banque de données à la recherche d'une correspondance. Comme cette technique est difficile à déjouer, elle est utilisée dans les sites à haute sécurité comme dans les centrales nucléaires ou les arsenaux.
2. *L'autorisation ou l'interdiction d'entrer ou de sortir* est le deuxième élément du système de contrôle d'accès et la conséquence de l'identification. Cette autorisation peut se traduire par le déclenchement automatique d'une entrée ou par une action humaine.

La procédure peut être effectuée sur place ou commandée à distance, à partir d'une centrale de contrôle.

Alarmes et détecteurs

L'alarme est le signal annonçant le danger ou attirant l'attention sur une anomalie. Elle permet de déclencher l'intervention qui s'impose. On a parlé à ce propos de surveillance «par exception»: quand tout est normal, chacun vaque tranquillement à ses occupations; soudain un incident est détecté et on est mis en état d'alerte. La sirène fait sursauter les malfaiteurs; ils se sentent enfermés comme dans une bulle de bruit qui les empêche de ne rien entendre d'autre. C'est pourquoi, la plupart des individus mal intentionnés qui déclenchent une alarme fuient sans demander leur reste. Sur le site d'une organisation, le déclenchement d'une alarme peut être suivi d'une intervention fort rapide.

Il est possible de distinguer dans un système d'alarme trois éléments:

1. *Des détecteurs ou capteurs* utilisent des systèmes électromagnétiques, des micro-ondes, des rayons X, des cellules photo-électriques, des ultrasons, etc. pour détecter les mouvements, les ouvertures de portes ou de fenêtres, les chocs, les vibrations, les bruits, des variations dans l'intensité lumineuse, la fumée, des explosifs, les perturbations d'un champ électrostatique, etc. On protège un périmètre par des capteurs installés aux portes, aux fenêtres, sur les murs, sur les clôtures, sous le sol, sur les toits et sur un objet, par exemple, un tableau ou un coffre-fort. Des capteurs peuvent balayer un espace pour y détecter les mouvements.
2. *Le système de contrôle d'alarme.* Dans les entreprises possédant un système d'alarme élaboré, le poste de contrôle a pour fonctions de recevoir les signaux émis par les capteurs, de traiter l'information, d'effectuer les discriminations nécessaires et d'envoyer des instructions. Les systèmes modernes possèdent générale-

ment des algorithmes de détection qui empêchent le déclenchement d'alarmes intempestives.
3. *Un signal.* L'alerte est donnée par une sonnette, une sirène, des lumières ou un voyant lumineux.

2 Les technologies dans les stratégies du délinquant et du chef de la sécurité

Dans un aéroport, une banque ou dans toute entreprise qui s'est dotée d'un service interne de sécurité, deux catégories d'acteurs s'opposent: les délinquants et les membres de l'équipe de sécurité. Ces derniers mettent en place un dispositif conçu pour faire reculer les premiers. De leur côté, les délinquants chercheront à déjouer le système de protection. À leur tour, les gens de la sécurité voudront mettre leur dispositif à l'abri de ces manoeuvres.

Les contre-mesures sont les moyens découverts par les délinquants pour atteindre leurs fins malgré les mesures destinées à les en empêcher. Il est utile ici d'en présenter quelques-unes.

- Les délinquants vont sévir ailleurs, dans les lieux mal protégés. C'est le déplacement.
- Ils trouvent la faille du système de protection et s'y engouffrent. Par exemple, ils découvrent l'angle mort des caméras de surveillance à l'abri duquel ils peuvent opérer sans être vus. (Voir les brèches dont parle KILLIAS 2001).
- Ils neutralisent un appareil, par exemple, ils désamorcent le système d'alarme, ou encore, dans un magasin, ils arrachent l'étiquette magnétique de l'objet qu'ils veulent voler.
- Ils spéculent sur l'inattention et la passivité du personnel de sécurité. C'est ainsi qu'ils vont tenter de faire sortir un objet volé dans un magasin muni d'un système de surveillance électronique en se disant que même si la sonnerie se déclenche, ils ne seront pas fouillés.

Il serait surprenant que des délinquants ne découvrent tôt ou tard l'une ou l'autre de ces contre-mesures. En effet, dans un lieu fréquenté par un grand nombre de personnes, il devrait se trouver au moins un petit malin qui imaginera le moyen de déjouer le dispositif de prévention. Par la suite, cet individu sera imité. C'est à cette étape que l'initiative du responsable de la sécurité vient prendre le pas sur la technologie. S'il est vigilant, il découvrira le pot aux roses et mettra au point des contre-contre-mesures.

Les détournements d'avions: 1962–2005

L'histoire récente des détournements d'avions fournit un exemple de ce cycle prévention –> contre-mesures –> contre-contre-mesures. Les fluctuations des détournements et des ripostes à ces crimes entre 1962 et aujourd'hui se sont succédées en sept étapes (les données sont tirées de l'ouvrage de WILKINSON 1986: 225–258).

- Première étape. Durant les années 60, les autorités de l'aviation civile enregistrent dans le monde un nombre croissant de détournements d'avions. Le point culminant est atteint en 1969: 70 détournements réussis et 12 tentatives. Les lignes aériennes américaines sont particulièrement frappées: 40 attentats.
- Deuxième étape. La riposte est internationale mais elle est particulièrement vigoureuse de la part des Américains. La mesure préventive principale prend la forme de fouilles pré embarquement utilisant des détecteurs de métaux et le filtrage des passagers. Ces contrôles sont rendus obligatoires aux États-Unis en 1973.
- Troisième étape. On enregistre une forte baisse des détournements d'avions. En effet, durant les cinq années allant de 1968 à 1972, on comptait 147 détournements (réussis ou non). Durant les cinq années suivantes (1973 à 1977), ce chiffre tombe à 32. Par la suite le nombre de détournements oscille autour de 12 par année.
- Quatrième étape. Les contrôles pré embarquement se relâchent, particulièrement sur les lignes intérieures.

- Cinquième étape. Attentats du 11 septembre 2001. Les terroristes d'Al-Qaida embarquent dans les vols domestiques armés de «cutters» ou de couteaux. À l'aéroport de Boston, dix terroristes passent l'examen du détecteur de métal et les rayons X sans éveiller les soupçons. À Washington, deux pirates de l'air déclenchent l'alarme. Les gardes les fouillent alors mais, curieusement, ils les laissent passer. (The 9/11 Commission Report 2004).
- Sixième étape. La mobilisation gigantesque qui a suivi ces attentats est bien connue. Les mesures de prévention sur lesquelles je voudrais attirer votre attention sont celles-ci: renforcement des contrôles de pré embarquement; installation d'une porte blindée séparant les passagers du cockpit de pilotage, cette porte restant verrouillée pendant le vol; formation des agents de sécurité; utilisation de détecteurs d'explosifs et d'appareils de radioscopie.
- Septième étape. Depuis, aucun autre attentat semblable à ceux du 11 septembre n'a été perpétré. Cependant nous savons que le réseau d'Al-Qaida dirige ses attaques ailleurs, notamment en Irak.

Cette succession d'actions des pirates de l'air suivies de réactions des responsables de la sécurité aérienne peut être schématisée de la manière suivante.

3 Les pirates de l'air – les acteurs de la sécurité

Il paraît évident ici que les attentats mobilisent les acteurs de la sécurité et que les mesures de prévention font reculer les criminels. Dans l'exemple précis que nous avons sous les yeux, le phénomène ne paraît pas surprenant. Cependant se pourrait-il que nous soyions en présence d'une dynamique assez générale? Se pourrait-il que, quand des attentats graves deviennent trop fréquents, les réactions qu'ils suscitent les fassent baisser? Si de tels processus existent, nous sommes devant un phénomène important qui n'a pas été vraiment pris en compte par les théories en criminologie. La théorie des brèches de KILLIAS (2001: 334) paraît ici comme une exception.

Il faut aller chercher ailleurs qu'en criminologie la manière de penser nous permettant d'appréhender ce genre de processus. Une évidence première de la pensée stratégique, c'est que, lors d'un affrontement, l'action d'un adversaire ne peut pas ne pas influencer l'autre. Une armée attaquée ne peut pas faire comme si elle ne l'était pas. Elle doit se défendre, contre-attaquer ou capituler. À son tour la contre-attaque force le premier agresseur à se défendre. Chacun fait la loi de l'autre pour écrire comme CLAUSEWITZ. Si nous raisonnons de cette manière et si nous nous inspirons de l'exemple de la piraterie aérienne, il se pourrait que la séquence suivante soit assez générale.

- Première étape, une forme de criminalité grave apparaît et gagne en fréquence si elle rencontre une résistance trop molle.
- Deuxième étape, quand l'activité criminelle atteint un niveau insupportable, la riposte monte en puissance.
- Troisième étape, si cette riposte est bien ajustée, la criminalité visée recule.
- Quatrième étape, cette réduction conduit les acteurs de la sécurité à baisser la garde.
- Cinquième étape, ceux-ci sont pris par surprise quand apparaît une nouvelle manifestation criminelle (ceci nous fait retourner à la première étape du cycle).

Cette logique d'action aide à comprendre pourquoi les technologies ne vont pas sans effet pervers. J'en vois deux. Le premier est la tendance à se reposer sur des appareils au point de cesser d'être vigilant et réactif. On se décharge sur la technologie du contrôle d'accès en négligeant de réagir, comme on l'a vu le 11 septembre 2001. On installe un système de télésurveillance, mais quand une infraction est observée sur un moniteur, on ne dispose pas de la capacité d'intervenir. Cette confiance excessive dans la technique est particulièrement marquée quand celle-ci est efficace. Or le recul de la criminalité suite à la mise en place de mesures de protection est un fait couramment observé. Le reflux de la piraterie aérienne après les mobilisations dont il vient d'être question n'est donc pas exceptionnel.

Cependant, précisément à cause de l'efficacité du dispositif, l'on a trop souvent tendance à s'y fier. La vigilance tombe alors. Tôt ou tard, quelques agresseurs coriaces découvriront une faille, très souvent humaine, dans le dispositif. C'est dire qu'une technologie de prévention reste toujours susceptible d'être déjouée, contournée, testée, percée. Et cette possibilité est d'autant plus forte que le système est passif. Une prévention vraiment efficace exige que les appareils soient soutenus par la vigilance pour détecter les stratagèmes, par l'imagination pour découvrir les correctifs et par la force pour neutraliser les agresseurs. Bref, en sécurité, les appareils ne sont des substituts ni à l'intelligence ni à l'action.

Il arrive aussi que les technologies fassent écran entre les acteurs de la sécurité, d'un côté, et les citoyens et contrevenants, de l'autre. Quand les policiers ont cessé de patrouiller à pied pour s'enfermer dans leur automobile, ils ont perdu de nombreuses occasions d'entrer en contact avec les gens. Et depuis la mise en place des systèmes d'appels téléphoniques avec un numéro facile à mémoriser, les policiers n'ont cessé de courir d'un appel à l'autre sans disposer du temps nécessaire pour comprendre les problèmes et encore moins pour les régler (DUPONT 2001). Avec la télésurveillance, les systèmes d'alarme et les contrôles d'accès automatiques, la présence physique d'un policier ou d'un garde n'est plus nécessaire. En cas d'infraction, l'intervention humaine devient donc incertaine et tardive. De tels appareils éloignent les intervenants des délinquants.

Intégration et synergie

Que nous apprennent les recherches évaluatives sur l'efficacité d'une seule mesure préventive comparée à un ensemble intégré de méthodes différentes? Dans certains cas, une seule intervention bien adaptée suffit (voir par exemple, WEBB 1997; DI LONARDO 1997; BARCLAY et coll. 1997; MASUDA 1997). D'autres fois, cela prend une combinaison de mesures complémentaires pour avoir raison d'un

problème criminel (PEASE 1997; TILLEY 1993; ANDERSON et coll. 1995; HANMER et coll. 1999; FARRELL 2005; WEBB 2005). Quand vient le moment de protéger un établissement important et exposé à une diversité de menaces, une seule mesure paraît insuffisante; il vaut mieux intégrer une brochette de moyens.

L'intégration, c'est la coordination de diverses mesures humaines et techniques complémentaires. Cette intégration vise à produire un effet *de synergie,* à produire de la sécurité par l'action coordonnée de plusieurs éléments. La figure 2 qui suit illustre la manière dont cette intégration peut-être réalisée au sein d'une organisation ou sur un site.

On devine qu'un tel dispositif protégera très efficacement le site dans lequel il est installé, surtout s'il est conçu et opéré intelligemment.

Il importe d'insister sur la fonction d'intégration de la centrale de contrôle. C'est là que sont reçus et enregistrés les signaux qui émanent des systèmes de détection et des observations faites par le personnel. Ces messages font l'objet de vérification. Une opération peut être commandée à distance, par exemple en déclenchant une sonnerie, ou en ouvrant ou renfermant une porte. Il est aussi possible que, de la centrale, un intervenant soit dépêché sur place par faire évacuer les lieux, expulser un intrus, l'arrêter, le désarmer, apaiser deux individus qui se disputent, prodiguer les premiers soins à une victime, appeler la police, les pompiers, un médecin ...

La technologie fournit plusieurs outils servant à l'intégration. On trouve d'abord les moyens de communication permettant de retransmettre les signaux, de déclencher des actions à distance et de se parler par téléphone ou par radio émetteur-récepteur. Les ordinateurs munis de logiciels spécialisés permettent de discriminer parmi les signaux reçus et de guider la décision. D'autres logiciels sont très utiles pour l'analyse de problèmes criminels récurrents. Ils permettent

de les localiser, d'en analyser la fréquence, de découvrir des patterns, de les classer.

Il paraît utile de distinguer trois niveaux d'intégration:

- Premièrement, *l'intégration des mesures préventives.* La télésurveillance, la surveillance humaine, les contrôles d'accès, les systèmes d'alarmes, les opérations commandées à distance et les interventions préventives sont combinées et coordonnées les une avec les autres. La figure 2 en fournit une illustration.
- Deuxièmement, *l'intégration des fonctions de sécurité.* À elle seule, la prévention ne suffit pas à assurer la sécurité d'une organisation. *Le renseignement* paraît indispensable pour connaître les problèmes et orienter la recherche de solutions. *La répression* s'avère nécessaire, par exemple, quand un individu passe outre aux mesures de prévention et commet un délit. Enfin, *les mesures d'urgence* s'imposent pour éviter qu'une crise ne s'aggrave ou dégénère.
- Troisièmement, *l'intégration de la sécurité aux autres activités et finalités non sécuritaires d'une organisation.* Il va de soi que la sécurité doit s'harmoniser avec les autres fonctions d'une organisation. Dans une usine, les ouvriers apprécient de se sentir en sécurité, mais leur tâche première, c'est de produire. Dans un hôpital, l'essentiel pour les patients, c'est d'être soignés. Il importe donc de distinguer, d'une part, les fonctions principales d'une organisation et, d'autre part, la sécurité. Il est évident que cette dernière doit être subordonnée aux premières. Les gens qui fréquentent un lieu devraient pouvoir vaquer à leurs occupations sans d'être dérangés; circuler sans être contrôlés à tout moment; agir et parler sans être surveillés. Un équilibre devrait donc être trouvé entre les contraintes de la sécurité et les fonctions premières de l'organisation.

La contribution à la sécurité du personnel qui n'est pas spécifiquement affecté à la sécurité est une autre dimension de cette intégration. Dans un magasin, le vendeur ne devrait pas laisser le voleur vo-

ler en toute quiétude. Le concierge d'un immeuble devrait verrouiller les portes qui doivent l'être.

Pourquoi un éventail intégré de mesures sécurise-t-il mieux un site qu'une mesure isolée? Quatre raisons viennent à l'esprit:

1. *L'intensité.* En combinant plusieurs mesures, l'action de sécurité peut atteindre un niveau d'intensité suffisant pour faire reculer la grande majorité des délinquants potentiels. Il est vrai que la seule vue d'une caméra de surveillance fera détaler les petits voleurs pusillanimes. Cependant les voleurs déterminés ne se laisseront pas arrêter si facilement. Plus on accumule sur leur chemin les difficultés et les risques, plus ils seront portés à se décourager.
2. Contre une diversité de menaces, on oppose différentes parades.
3. *L'étanchéité.* Plusieurs mesures combinées peuvent assurer une protection assez étanche d'un site contre les intrusions, les vols, les fraudes et les violences.
4. *La discrimination et l'adaptation fine des réponses aux problèmes.* Des détecteurs d'alarme couplés à des caméras de surveillance permettent à un préposé de vérifier visuellement si l'anomalie détectée appelle une réponse et laquelle. La nature exacte d'un problème de sécurité ne peut être saisie et comprise qu'en combinant plusieurs informations provenant de sources différentes.

4 Conclusion: un rôle pour les criminologues

À la question posée dans mon introduction, les développements qui précèdent m'autorisent à répondre: oui les nouvelles technologies de la sécurité préviennent la criminalité dans les sites où elles sont correctement mises en place. Un directeur d'un service interne de sécurité compétent est bien placé pour accomplir sa mission. Faisons un pas de plus. Dans les pays occidentaux, les organisations privées, publiques et parapubliques dotées d'une sûreté interne sont nombreuses et importantes. C'est dire qu'un nombre considérable de personnes, de richesses et d'espaces sont sécurisés par ces services internes. Il

est donc permis de conclure que la contribution à la baisse de la criminalité globale des responsables de la sécurité interne utilisant les nouvelles technologies est loin d'être négligeable.

Ceci nous laisse entrevoir un rôle pour le criminologue. Quel autre professionnel qu'un criminologue est mieux préparé pour devenir le responsable de la sécurité au sein d'une organisation? Qui peut mieux que lui analyser les problèmes criminels se posant au sein de cette organisation? Qui peut mieux que lui adapter les mesures préventives à l'évolution des tactiques délinquantes et les combiner les unes aux autres pour produire un effet de synergie? Car c'est le criminologue qui est préparé à analyser les problèmes criminels et qui peut concevoir un système intégré de mesures de sécurité. Quel autre professionnel que lui pourrait mettre en synergie la connaissance du crime et celle des solutions; la prévention et la répression?

Références

ANDERSON, D., PEASE, K. (1997). *Biting back: Preventing Repeat Burglary and Car Crime in Huddersfield,* in CLARKE, R.V. (ed.), *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Guilderland, N.Y.: Harrow and Heston.

BARCLAY, P., BUCKLEY, J., BRANTINGHAM, P. J., BRANTINGHAM, P. L., WHIN-YATES, T. (1997). *Preventing Auto Theft in Commuter Lot: A Bike Patrol in Vancouver,* in CLARKE, R.V. (ed.), *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Guilderland, N.Y.: Harrow and Heston.

DILONARDO, R. (1997). *Defining and measuring the economic benefit of electronic article surveillance*, in CLARKE, R.V. (ed.), *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Guilderland, N.Y.: Harrow and Heston.

DUPONT, B. (2001). *Policing in the information age: Technological errors of the past in perspective,* in ENDERS, M.; DUPONT, B. eds. *Policing the Lucky Country.* Sydney: Hawkins Press.

FARRELL, G. (2005). *Progress and prospect in the prevention of repeat victimization*, in TILLEY, N. ed. *Handbook of Crime Prevention and Community Safety.* Cullompton, Devon: Willan.

FELSON, M. (1998). *Crime and Everyday Life,* 2nd edition. Thousand Oaks, California: Pine Forge Press.

HANMER, J., GRIFFITHS, S., JERWOOD, D. (1999). *Arresting Evidence: Domestic Violence and Repeat Victimisation.* London: Home Office; Policing and Reducing Crime Unit.

KILLIAS, M. (2001). *Précis de criminologie,* 2ème édition. Staempfli, Berne.

LEMAN-LANGLOIS, S., BRODEUR, J.-P. (2005). Les technologies de l'identification. Une note de recherche. *Revue internationale de criminologie et de police technique et scientifique.* n. 1, pp. 69–82.

MASUDA, B. (1997). *Reduction of Employee Theft in a Retail Environment: Displacement vs Diffusion of Benefits,* in CLARKE, R.V. (ed.), *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Guilderland, N.Y.: Harrow and Heston.

PEASE, K. (1992). *Preventing Burglary on a British Public Housing Estate,* in CLARKE, R.V. (ed.), *Situational Crime Prevention: Successful Case Studies*. New York: Harrow and Heston. 223–229.

THE 9/11 COMMISSION (2004). *Final Report of the National Commission on Terrorist Attacks upon the United States.* New York: Norton, Kean, T.H. Chair.

TILLEY, N. (1993). *Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities.* London: Home Office. Police research group. Crime prevention paper no 42.

WALSH, T. (1995). *Protection of Assets. Santa Monica,* CA. Merritt Co.

WEBB, B. (1997). *Steering Column Locks and Motor Vehicule Theft: Evaluation from Three Countries,* in CLARKE, R.V. (ed.), *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Guilderland, N.Y.: Harrow and Heston.

WEBB, B. (2005). *Preventing vehicle crime.* In TILLEY, N. ed. *Handbook of Crime Prevention and Community Safety.* Cullompton, Devon: Willan.

WILKINSON, P. (1986). *Terrorism and the Liberal State.* London: Macmillan.