L'analyse de problèmes de sécurité et la conception de solutions adaptées

(2007) Stéphane Leman-Langlois
M. Cusson, B. Dupont et F. Lemieux, Traité de sécurité intérieure, Montréal, Hurtubise HMH (367-386).

Résumé

Ce chapitre décrit trois niveaux d'analyse des problèmes, chacun accompagnés de types de solutions appropriées. Il ne s'agit pas de recommander des solutions ou même des approches des problèmes, puisqu'un des arguments principaux est que chaque situation diffère des autres par certains détails qui sont toujours d'importance — détails qui deviennent particulièrement utiles au stade de l'élaboration de solutions.

Introduction

On a souvent l'impression que les problèmes de sécurité liés à des personnes, à des sites ou à des biens se manifestent naturellement à l'observateur un tant soit peu perspicace. En réalité, pourtant, si certaines failles manifestes tendent à l'évidence, comme les barrages hydroélectriques d'Hydro-Québec qui étaient ouverts à tous les passants en janvier 2005, la plupart des facteurs réduisant notre sécurité sont beaucoup moins faciles à identifier. Il y a donc lieu de poser un regard théorique et analytique sur la notion de problème, et plus précisément sur les activités qui consistent à identifier, comprendre, communiquer et remédier aux situations définies comme des problèmes de sécurité dûs à des actions humaines intentionnelles (donc, mis à part ceux qui proviennent des incendies accidentels, des accidents ou des inondations). Il sera question de la notion même de problème, des niveaux où des problèmes peuvent être identifiés et de l'importance des solutions disponibles dans l'identification des problèmes.

La conception de « problème » qui est utilisée ici ne différencie pas de manière fondamentale entre les problèmes privés, publics, entre ceux qui sont du ressort de la police et ceux qui concernent la sécurité privée, les institutions, les groupes ou les individus. Identifier un problème et y faire face, dans tous ces cas, procède des mêmes outils conceptuels. Même dans les cas où le problème est de nature criminelle, l'utilisation du système pénal doit être conçue comme *un outil parmi d'autres* permettant de solutionner certains problèmes, dans certaines situations. C'est d'ailleurs un des outils les moins efficaces pour faire diminuer les problèmes de criminalité (Clarke et Eck, 2003 : ch. 4). En pratique, avoir à surveiller et à arrêter, à répétition, *ad vitam eternam*, une suite toujours renouvelée de délinquants, est une tâche assommante, ni efficace, ni efficiente, et qui porte à des conséquences indésirables sous les angles social, individuel et commercial. Une telle réponse ne correspond pas à notre définition de *solution* à un *problème.*

L'identification d'un problème, pour avoir une utilité pratique, doit être adaptée aux caractéristiques de la personne et/ou de l'organisation qui en subit les conséquences et de celles de la personne et/ou organisation qui est responsable de le régler. L'approche analytique de la sécurité doit donc s'adapter à son « client », puisque les circonstances physiques, légales, économiques diffèrent radicalement, par exemple, entre les organismes communautaires locaux, les grands organismes gouvernementaux, les petites et moyennes entreprises qui remplissent nos parcs industriels et le citoyen moyen. Si les institutions gouvernementales peuvent s'intéresser aux problèmes généralisés qui affligent la société entière, ces derniers ne forment au contraire qu'un décor inaltérable pour la plupart des gens ordinaires. Par exemple, il est inutile d'annoncer au propriétaire d'un petit commerce que son problème de criminalité est causé par le mauvais fonctionnement du système d'éducation. La modification du système d'éducation étant hors de la portée et de la responsabilité de la petite entreprise, *il est inutile de l'identifier comme problème de sécurité*, même si c'est effectivement la cause principale de ses difficultés. Cela dit, nous verrons tout de même plus bas qu'il n'est pas approprié d'exclure d'emblée toutes les formes de prévention à caractère social de la sphère d'influence des acteurs non-gouvernementaux.

Le tableau 23-1 montre à quel point les contextes pouvant présenter des problèmes de sécurité sont variés. Identifier des problèmes est une tâche microscopique d'analyse spécifique. Il n'y a pas de ruban à mesurer les problèmes ni de recette de la sécurité : chaque nouvelle évaluation de sécurité est unique, différente des précédentes et des suivantes. Ainsi, ce que l'expert en sécurité doit développer n'est pas une encyclopédie des problèmes et des solutions, mais bien une façon de percevoir et une attitude propice à la résolution originale de situations spécifiques.

Tableau 23-1 : diversité des problèmes de sécurité

sites	« problèmes » typiques	impacts potentiels
• industriels • commerciaux • gouvernementaux • communautaires • personnes • espaces publics • espaces privés • espaces « privés de masse » • espaces virtuels • environnement	• vol de matériel • vol de services • vol d'informations • vol de devises • fraude • corruption • violence, intimidation • destruction • incivilités • sentiment d'insécurité	• pertes financières • hausse des primes d'assurances • responsabilité civile • diminution de la productivité • diminution de la compétitivité • réduction de la clientèle • dommages à la santé • perte d'informations • perte de la vie privée • désorganisation sociale • tensions interpersonnelles

1 Risques, menaces, vulnérabilités

Dans ce qui suit, les mots « risque », « menace » et « vulnérabilité » ont un sens précis et ne sont pas interchangeables. Je suivrai les définitions conventionnelles, qui ont cours dans la littérature spécialisée. Une **menace** est constituée par la présence d'éléments pouvant s'attaquer à la sécurité d'une organisation, d'un groupe ou d'une personne. Ces éléments comprennent bien sûr les menaces écologiques, météorologiques, celles qui viennent de la concurrence normale du marché (pour ce qui est des entreprises) et des accidents, mais comme je l'ai déjà mentionné, ce chapitre porte exclusivement sur les menaces humaines intentionnelles. Nous nous pencherons, dans une sous-section suivante, sur le fait que ces menaces soient de nature criminelle ou non et sur l'importance de cette distinction.

Les menaces sont d'une variété infinie, et *distribuées inégalement* c'est–à-dire que chaque site, organisme, groupe, individu, est exposé à un ensemble de menaces qui lui est particulier. Elles peuvent provenir de l'extérieur, c'est-à-dire d'individus, de groupes et d'organisations dont les activités sont indésirables pour l'entité qui doit être protégée. Pour un magasin à rayons, une menace classique est celle représentée par l'existence d'individus s'adonnant au vol à l'étalage. Pour un édifice gouvernemental, la menace peut provenir de citoyens manifestant à l'extérieur. Pour un réseau de transport en commun, elle peut provenir de citoyens préparant une attaque terroriste. Pour une compagnie d'assurance, il peut s'agir de clients qui tentent d'inclure dans leur formulaire de réclamation des dommages qu'ils n'ont pas réellement encourus. Un aéroport peut être paralysé par un canular au sujet d'une bombe.

Les menaces sont aussi *internes*, lorsqu'un membre de l'organisation ou autre groupe social se conduit d'une manière qui peut causer un tort au groupe. Pour une banque, il peut s'agir de gestionnaires qui détournent des fonds. Pour un ministère, il peut s'agir de fonctionnaires faisant un mauvais usage de banques de données officielles. Dans un hôpital, des employés peuvent voler des médicaments ou des équipements. Des professeurs d'université peuvent s'approprier du matériel informatique qui ne leur appartient pas.

Les **vulnérabilités** sont la contrepartie des menaces : ce sont les facteurs qui exposent personnes, biens et sites à des attaques potentielles. Une porte mal verrouillée, un faux plafond trop élevé et où on peut ramper, des murs fragiles, etc. sont des vulnérabilités typiques des édifices à bureaux ordinaires. Des réseaux informatiques mal sécurisés et des employés à qui on peut facilement soutirer leur code d'utilisateur sont des vulnérabilités très répandues dans la plupart des organisations (sans compter les failles technologiques : un *Blackberry* duquel on croit avoir effacé les données ne fait que les *cacher* à un utilisateur peu expérimenté et les conserve tout de même en mémoire jusqu'à ce que cette portion de la mémoire soit à nouveau requise — ou jusqu'à ce qu'un curieux aille les chercher). Un commerce est vulnérable au vol à l'étalage si ses rangées de tablettes sont trop étroites, mal éclairées, mal surveillées, trop loin du centre d'activité des employés qui pourraient les surveiller, etc. Un barrage hydroélectrique est vulnérable si l'accès à ses turbines est ouvert, si personne n'y monte la garde, etc. Un réseau de transport en commun est vulnérable si on ne fouille pas les passagers, si on n'identifie pas qui y entre et y sort, si on ne contrôle pas l'achat des billets et si on ne retire pas toutes les poubelles et autres contenants pouvant servir à cacher une bombe, etc. Ce dernier exemple souligne au passage qu'on ne peut, en aucun cas, viser à faire disparaître ou même contrôler *toutes* les vulnérabilités — surtout dans les lieux ouverts au public. L'invulnérabilité ne peut donc pas être le but d'un programme raisonnable de sécurité.

Le **risque** est la correspondance d'une vulnérabilité à une menace. Une porte déverrouillée constitue toujours

une « vulnérabilité », mais si vous vivez dans un village où personne n'est intéressé à entrer chez vous, elle n'engendre aucun *risque*. Que l'accès à un barrage hydroélectrique dans le grand Nord ne soit pas contrôlé ne constitue pas non plus un risque pour la sécurité — mis à part le « risque » que des orignaux aillent y brouter du lichen. Puisqu'il n'y a aucun malfaiteur désirant y entrer, cette vulnérabilité reste sans conséquence tangible sur la sécurité des lieux. Le risque, on l'aura compris, est donc une notion statistique, probabiliste : il s'agit d'évaluer la *probabilité* qu'une personne décide de tenter de profiter d'une vulnérabilité ; l'action humaine n'est pas déterminée, elle est contingente.

Dans bien des cas, cette évaluation est fondée sur le passé : si un commerce a connu une moyenne relativement stable de 17 vols à l'étalage par mois dans les 48 derniers mois, il est clairement à prévoir que le mois prochain comptera à peu près 17 vols à l'étalage. En obtenant des informations complémentaires on pourra également prévoir la valeur des pertes encourues, les caractéristiques des voleurs et celles des produits qui seront volés — et donc leur emplacement exact sur le plancher. On peut également prévoir à quelle heure, quel jour de la semaine les vols sont les plus probables. On sera alors en mesure de trouver un moyen adapté pour en faire la prévention.

Dans d'autres cas, l'évaluation des risques est beaucoup plus approximative. Par exemple, dans la planification de dispositifs de sécurité pour un édifice qui n'est pas encore construit ou pour ce qui est des événements très rares, comme le risque d'attaque terroriste. Dans le premier cas, il s'agit de risques conventionnels, mais qui n'ont pas encore été encourus par l'entité particulière qu'il faut protéger. Une évaluation relativement fiable du risque peut être réalisée en comparant l'édifice futur à d'autres de type, vocation et contexte géographique apparentés. Dans le second cas, l'évaluation du risque reste subjective. Les compagnies d'assurances ont des formules de calcul du risque d'événements rares, mais elles ne sont utiles qu'avec l'agrégation massive de leurs clients et servent uniquement à déterminer le coût de la prime qu'ils devront payer afin de compenser ou de minimiser les conséquences éventuelles de cet événement (ce qui ne constitue aucunement une *prévention*, bien sûr : au contraire, les assurances dédommagent, par définition, les clients qui n'ont pu se protéger efficacement). Les chiffres qui ressortent de ce genre de calcul sont très peu utiles dans l'analyse de problèmes spécifiques à une entité donnée (voir Ericson et Doyle, 2004).

Par ailleurs, il faut être bien certain de savoir distinguer le risque de son penchant opposé, l'*incertitude*. L'incertitude, bien que donnant également lieu à un certain sentiment d'insécurité et à un désir de se protéger, représente — contrairement au risque — ce que l'on *ne sait pas* au sujet du futur — donc, rationnellement parlant, il n'est pas possible de savoir comment s'en protéger et peu efficient d'engager des ressources pour le faire (on peut tout de même avoir des raisons politiques, idéologiques ou sociales de le faire quand même, pour rassurer le public. C'est alors un exercice symbolique, entièrement subjectif).

Enfin, la notion de « **problème** » mérite également une définition. Ni les risques, ni les vulnérabilités, ni les menaces — ni les crimes, d'ailleurs — ne sont des *problèmes*. Certains risques, à certaines conditions, peuvent devenir des problèmes et demander une intervention. Le rôle de l'analyste est de déterminer les critères permettant de passer en mode de « résolution de problème », exercice généralement fondé sur un calcul des pertes possibles. Le tableau 23-2 illustre la relation entre le risque, la gravité des conséquences ou de l'impact de la conduite indésirable (nommée « criticalité », *criticality*, dans certains ouvrages), et la notion de problème.

Tableau 23-2 : matrice typique d'évaluation des problèmes de sécurité

<table>
<tr><th>« RISQUE » ↱</th><th colspan="3">probabilité</th></tr>
<tr><td>conséquences</td><td>faible</td><td>moyenne</td><td>élevée</td></tr>
<tr><td>insignifiantes</td><td colspan="2">zone des « irritants »</td><td rowspan="3"></td></tr>
<tr><td>sensibles</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>graves</td><td colspan="2">zone des « problèmes »</td></tr>
</table>

Au sens pratique, exposer un problème c'est faire la description détaillée des menaces, vulnérabilités, des probabilités de méfaits et de la gravité de leurs conséquences éventuelles. En vue d'une solution, il faut y ajouter l'articulation logique d'une hypothèse quant aux actes particuliers qui pourraient s produire dans le futur, ainsi qu'au sujet des motifs qui sous-tendent la conduite des personnes qui les poseront. Par exemple, un risque d'espionnage industriel ne deviendra un « problème », au sens pratique, que lorsqu'on l'aura mis en contexte précis : quels sont les secrets industriels qui doivent être protégés, sous quelle forme se présentent-ils, qui a besoin d'y avoir un accès légitime, qui pourrait vouloir les voler et pourquoi, quelle est la durée de la vie utile de ces secrets, combien de temps

faudrait-il à un concurrent ou une personne mal intentionnée pour profiter de ces secrets (ce temps dépasse-t-il leur vie utile), quelles seront les conséquences pour l'organisation de la subtilisation de ces secrets, etc.

Enfin, il faut noter qu'une matrice comme celle présentée au tableau 23-2, bien qu'extrêmement répandue dans la littérature sur la sécurité (presque tous les ouvrages en ont une version ou une autre. Par exemple, Broder, 2000 : 24 ; Fischer et Green, 2004 : 141 ; Johnson, 2005 : 351), tend à donner une importance démesurée aux impacts qui peuvent être traduits en valeur monétaire. La version offerte par Broder (2000 : 24) calcule *uniquement* la valeur financière des impacts. C'est une approche héritée des compagnies d'assurance, qui a certes sa place dans plusieurs contextes mais qui doit être prise comme un outil conceptuel et non comme un modèle à suivre.

2 Comment reconnaître un problème

On peut avoir l'impression que certains problèmes sont immédiatement évidents à l'expert en sécurité faisant son inspection. À simplement visiter les lieux, il apercevra tout de suite les racoins mal éclairés où peuvent se dissimuler les malfaiteurs, les portes, clôtures et autres contrôles d'accès insuffisants, le manque de gardiens physiquement présents ou surveillant à l'aide de caméras, etc. On pourrait appeler cette approche « empirique », non pas au sens scientifique, mais bien au sens où elle provient de l'expérience subjective de l'inspecteur. Or, ceci est nettement insuffisant et une approche plus rigoureuse donnera des résultats beaucoup plus clairs. Un des défauts de l'approche empirique est de cantonner l'inspecteur dans les recettes habituelles. Un expert des caméras en circuit fermé, par exemple, analysera les lieux en fonction de la présence et de l'efficacité de caméras installées — alors que les problèmes spécifiques aux lieux sont peut-être d'une nature invisible aux caméras. Adopter une approche plus objective s'impose donc.

Ici, une courte digression est nécessaire. Souvent l'inspecteur/expert en sécurité n'est pas libre de tout conflit d'intérêt. C'est le cas d'experts qui, au-delà de l'évaluation de la sécurité des lieux, sont aussi entrepreneurs en services de sécurité (souvent oublié, cet aspect est tout de même mentionné dans Broder, 2000 : 223). Dans ce cas exemplaire, l'inspection ne vise pas seulement l'identification de problèmes mais bien la vente de services. C'est, au-delà et potentiellement au détriment d'une analyse rigoureuse, une opportunité commerciale. On ne s'étonnera pas de constater que ces experts découvrent une foule de problèmes auxquels, par pure coïncidence bien sûr, leur entreprise peut remédier.

La phase « pré-problème »

Il s'agit du point de départ de l'analyse. Pourquoi est-on là en train de vérifier les accès ou de demander aux personnes leur opinion sur leur sécurité ? L'élément déclencheur du processus d'évaluation de la sécurité a un effet profond sur le déroulement ultérieur des activités et sur le choix des solutions.

Plusieurs points de départ sont possibles, dont trois types principaux. Premièrement, dans un grand nombre de cas l'expert en sécurité est *appelé* sur les lieux d'un problème déjà défini par ceux qui recourent à ses services. Un policier est confronté aux revendications de résidents d'un quartier ou aux demandes de ses supérieurs qui ont identifié une statistique qu'ils jugent nécessiter une intervention. Un expert-conseil est engagé pour trouver un remède à une série de vols dans un entrepôt.

Les personnes qui font appel à l'expert sont elles-mêmes des sources importantes d'information et des acteurs sociaux capables d'analyser les situations qui les entourent. Ainsi, leur conclusion qu'un phénomène est « problématique » est utile, qu'ils soient eux mêmes experts en la matière ou simples citoyens. Par contre, il est courant pour ces acteurs de commettre un certain nombre d'erreurs assez typiques. La première est de sous- ou surévaluer le risque que représentent les situations pour la sécurité parce qu'ils ne disposent pas de moyens de comparer leur environnement quotidien à d'autres environnements, bref de contextualiser les faits. La seconde est de donner une importance disproportionnée à certains événements ayant marqué leur mémoire, tout en ignorant leur prévalence statistique réelle. Par exemple, il faut s'attendre à ce que des gens mis au courant d'une attaque particulière dans un stationnement concluent immédiatement que ce genre d'attaque est fréquent alors qu'en fait il est exceptionnel — c'est son caractère exceptionnel, justement, qui le rend si saillant. Au contraire, en termes d'analyse statistique, le *risque réel* d'une telle attaque serait, dans cet exemple fictif, extrêmement faible (il s'agit en fait d'un incident isolé). L'exemple de l'attaque au collège Dawson, en septembre 2006, illustre : des citoyens réclamèrent aussitôt un contrôle plus strict des armes à feu, l'installation de détecteurs de métal aux entrées des écoles, et les journalistes introduisaient leurs reportages par les mots, « encore une fois » ; or, ce genre d'attaque, bien qu'horrible, est extrêmement rare (la dernière remonte à 1989, dans un autre établissement bien sûr). Troisièmement, mentionnons brièvement que des raisons *illégitimes* peuvent être à la source de la consultation d'un expert : par exemple, l'administration d'une entreprise peut tenter de transformer en déviance de ses employés des problèmes de sécurité au travail qui sont en fait reliés au mauvais fonctionnement de ses équipements, afin de se déresponsabiliser.

La première tâche de l'évaluateur de la sécurité est donc de définir indépendamment la nature de la situation qui lui est soumise. Il est donc possible que cette définition diffère de celle de ses clients — situation qui requerra un certain doigté dans la présentation de son rapport. Si l'expert résout ce dilemme en installant un système qui, selon toute analyse rationnelle, sera *inutile* mais sur lequel le client insiste, il faudra clairement et explicitement noter ceci et avertir à l'avance que l'évaluation de l'intervention, qui est une étape cruciale du modèle de prévention par résolution de problème, ne sera pas positive (par exemple, l'installation de détecteurs de métal au collège Dawson susmentionné, alors que l'attaque débuta à l'extérieur de l'édifice).

Le second type de point de départ d'une évaluation en sécurité est celui où la cible 1) n'est pas encore implantée ou 2) est implantée dans un environnement en transformation imminente (par exemple, un organisme communautaire désire connaître l'impact qu'aura la construction éventuelle d'un complexe sportif ou d'un casino sur la sécurité d'un quartier). Dans ces deux cas, l'évaluation du risque est entièrement *théorique*, au sens où elle procède d'une série d'hypothèses sur 1) la position future de la cible, 2) le mode et la rapidité du changement environnemental et sa forme finale. Dans ces cas les problèmes ne sont pas déterminés à l'avance, il faut les identifier. Généralement, on procède par analogie : à quelle autre situation celle-ci ressemble-t-elle ? Un inventaire de situations analogiques doit être dressé, à partir duquel on précédera à la même collecte d'information décrite ci-dessus.

Le dernier type d'enclenchement d'une évaluation est le cas de ce que nous pourrions appeler la « responsabilité continue ». Il y en a deux illustrations assez courantes, celle du cadre responsable de la sécurité d'une organisation et celle de la police. Dans les deux cas, l'analyse de problème s'inscrit dans un effort continu d'assurer une sécurité ou une qualité de service maximisées. Il est presque certain que les problèmes principaux sont non seulement déjà identifiés, mais qu'un ensemble de mesures ont déjà été prises pour tenter de les contrôler. L'information de base est relativement plus facile à trouver, et l'analyste dispose en plus des résultats des solutions déjà tentées ou en cours.

Analyser la situation

Une approche rigoureuse de toute situation nécessite en tout premier lieu à obtenir des informations suffisamment détaillées sur le contexte social et géographique des lieux, personnes, espaces ou espaces virtuels à protéger — ceci, de deux façons principales. La première consiste à effectuer une collecte systématique d'informations pertinentes déjà disponibles, comme par exemple des statistiques sur les pertes, sur les activités des individus, et des descriptions d'événements et de phénomènes moins tangibles (la peur du crime de résidents d'un quartier, par exemple). Ces informations peuvent être disponibles dans diverses institutions, dont la police, les compagnies d'assurance, les organismes communautaires et les institutions de recherche scientifique comme les universités. Souvent, les organisations colligent leurs propres statistiques — à l'occasion ce sont justement ces statistiques, jugées alarmantes, qui sont la raison pour laquelle on a fait appel à un expert-évaluateur de la sécurité.

La seconde forme de collecte est l'approche expérimentale : il s'agit, dans les cas où l'information disponible est inadéquate ou inexistante, d'ajouter une étape préliminaire spécifiquement vouée à l'observation du terrain. Par exemple, si on fait face à une problématique identifiée de prostitution dans un quartier, sachant que les statistiques policières sont généralement déficientes dans ces cas (c'est un crime typiquement peu rapporté à la police), il faut prévoir une période d'observation systématique. Ceci permettra de mieux comprendre la situation. Typiquement, il faut disposer d'informations sur 1) les endroits physiques, 2) le déroulement chronologique des phénomènes, 3) la méthodologie, 4) les objectifs probables, 5) les victimes et 6) les caractéristiques sociales de l'endroit où ont lieu les faits à l'étude. Dans un second temps, il faut savoir organiser ces informations en un tout intelligible, sous forme de cartes, de séries chronologiques, de tableaux comparatifs appropriés. La capacité d'organiser ainsi l'information est souvent négligée par les professionnels, qui se fient à leur expérience pour relever les données intéressantes. C'est insuffisant, peu rigoureux et surtout, peu favorable au développement d'approches novatrices en matière de sécurité.

Une fois les informations collectées, il faut savoir les rendre utiles, en fonction de l'objectif d'intervention qui est fixé — l'exercice ne vise pas simplement à satisfaire la curiosité, mais bien à modeler une solution adéquate. En effet, ni l'observation, ni la mesure d'un fait ne révéleront sa signification : il faut savoir interpréter. Par exemple, placer des points sur une carte électronique peut révéler des concentrations de criminalité dans un quartier, mais il reste encore à comprendre *pourquoi* les crimes sont commis à ces endroits. Si c'est un simple hasard, il n'y a pas de raison de supposer que cet endroit continuera d'être « chaud » dans le futur. C'est pourquoi plusieurs organisations de police n'arrivent pas à tirer profit de logiciels de géomatique comme *MapInfo*, qui sont de puissants outils d'analyse, mais qui ne font pas eux-mêmes l'analyse des données (Willis, Mastrofki et Weisburd, 2003).

Pour analyser, des êtres humains adéquatement formés doivent réfléchir aux données des faits identifiés, ce qui veut dire les approcher avec une logique rigoureuse, à la fois déductive et inductive. Déductive, au sens où l'analyse forme des hypothèses et les vérifie en se rapportant aux faits connus ; inductive, lorsque des hypothèses sont formées à partir de l'information disponible. Prenons un exemple cité dans Shearing (2000 : 204-205), où un

directeur de la sécurité doit répondre à des vols d'outils électriques dans une grande entreprise canadienne. Plusieurs outils disparaissent et les pertes commencent à être importantes. Une première déduction est qu'il est possible qu'un ou un petit groupe d'employés volent les outils pour les revendre. Cette hypothèse est écartée puisque après vérification, les faits montrent que les outils disparaissent à l'unité, et à la veille des week-ends. Il semble donc que les coupables risquent d'être des employés ordinaires, utilisant ces outils pour travailler chez eux et non pour en faire le trafic. On voit donc l'importance de disposer d'informations précises sur les situations à analyser. Le tableau 23-3 dresse une liste des principales informations cruciales.

Tableau 23-3 : aspects des situations sur lesquels il faut disposer d'informations détaillées

matériel	**humain**	**géographique**	**temporel**
ce qui a été volé/endommagé. Inclue services et informations (sites sur la toile, informations confidentielles, etc.)	dommages faits aux personnes, incluant dommages psychologiques et relationnels ; état des relations interpersonnelles	où les actes ont-ils eu lieu/risquent-ils d'avoir lieu; comparaison avec d'autres lieux équivalents. Inclue localisation sur une carte et sur les plans d'un édifice/site	à quelle heure, quel jour les actes ont-ils lieu ; y a-t-il une variation saisonnière, une coïncidence avec d'autres événements, etc.

Comme nous le verrons dans un instant, cette conclusion eut un impact profond sur la solution trouvée au problème. Au départ, le directeur de la sécurité avait songé à placer des caméras pour démanteler le réseau de voleurs et les traduire en justice. En sachant que des employés ordinaires étaient responsables, cette solution parut inacceptable : 1) ces employés ont coûté cher à former et sont compétents ; 2) ce genre d'approche, mettant tous les employés sous surveillance, créerait un climat de suspicion et nuirait aux relations de travail, au moral des employés et pourrait réduire la productivité et durcir les relations avec le syndicat ; 3) il n'y a pas de raison de croire que les employés qui remplaceraient les coupables seraient moins disposés à voler les mêmes équipements.

Les niveaux de problèmes

Un problème, somme toute, n'est rien de plus que l'*articulation logique d'un état de fait tel que perçu par un acteur social donné comme méritant d'être corrigé*. Les acteurs sociaux étant situés dans différents contextes sociaux, organisationnels, économiques, etc., on ne doit pas se surprendre de constater que chacun voit les problèmes à des endroits différents. Dans le début d'histoire citée ci-dessus, les *faits* sont incontournables : des outils disparaissent. Il sont de tel type, ils disparaissent à telle fréquence, à tel jour de la semaine et ils ont une valeur *x*. Par contre, alors qu'un individu y verra un problème de criminalité ou de contrôle des déplacements physiques sur le site, un autre y verra un problème plus large de besoins individuels se déployant dans un certain contexte de relations industrielles. Qui a tort ? Ni l'un ni l'autre : il y a effectivement des actes criminels commis, qu'on pourrait sans doute contrôler avec des caméras ou des mouchards électroniques (de type RFID, entre autres) collés sur les objets convoités. Il y a pourtant aussi des êtres humains évoluant dans une structure organisationnelle et sociale donnée. Ainsi, sans se tromper, on peut voir un problème sous divers angles, ou à divers « niveaux » de complexité variable.

Le premier niveau est celui de l'environnement physique immédiat. Essentiellement, ce type de définition du problème fait abstraction des *raisons* qui motivent les acteurs causant un tort et se concentre sur les éléments qui rendent leur conduite dommageable physiquement possible. Ces éléments facilitateurs sont de deux ordres : 1) une surveillance inadéquate ; 2) une protection physique inadéquate. Remédier à un de ces aspects peut souvent faire disparaître l'autre. Par exemple, la protection physique de produits sur un étalage (par divers mécanismes tous plus ingénieux les uns que les autres) réduit la nécessité de surveillance directe des lieux, et vice-versa. Le choix d'une approche sera dicté surtout par la question des coûts relatifs des deux solutions.

Comme on l'a remarqué souvent en criminologie (et plus spécifiquement chez Cohen et Felson, 1979), le nombre des infractions liées à l'appropriation de biens et services est fortement dépendant de la présence de personnes les surveillant et, bien sûr, des opportunités créées par l'abondance des biens et services en question (de biens *mobiles* et de services automatisés, bien sûr ; on vole rarement les maisons ou les mises en plis). Le tableau 23-4 donne une courte liste d'exemples de facteurs facilitateurs et de tactiques permettant d'y remédier.

Comme on le voit, la solution tactique est souvent relativement facile à trouver, puisqu'une fois le problème bien posé, elle coule de source : elle est fondée sur les capacités anatomiques et physiologiques de l'être humain (pensez à la manière dont sont conçues les trappes des machines distributrices de boissons) et sur l'élément de dissimulation qui est intrinsèque à l'usage illégitime d'un bien ou service (il est difficile de profiter illégitimement d'un bien à la vue de tous — ou du moins à la vue de son propriétaire). Le mode précis d'implantation de ces solutions peut être extrêmement complexe, comme l'installation de centaines de caméras et du matériel nécessaire à leur

surveillance dans une grande entreprise, mais l'effort conceptuel liant un problème de visibilité à la solution des caméras, par exemple, reste élémentaire.

Tableau 23-4 : vulnérabilités environnementales et réponses tactiques

informationnels	**personnels**	**physiques**	
lignes téléphoniques, réseaux informatiques non sécurisés ; copies de sauvegarde non protégées et/ou non cryptées	mode de sélection et de surveillance du personnel défaillant ; absence de formation continue, en particulier pour les prémunir contre l'ingénierie sociale ; formation défaillante du personnel dédié à la sécurité	*déplacements* points d'accès (de l'extérieur, entre les zones intérieures) insuffisamment contrôlés ; objets et services (par exemple espace sur un serveur, réseau de distribution électrique) facilement amovibles ou exploitables	*visibilité* facilité de dissimuler les objets et personnes ; endroits sans surveillance ou peu fréquentés ; endroits peu éclairés, retirés ; endroits voisins permettant de préparer un méfait
réponses tactiques conventionnelles			
sécurisation et surveillance des réseaux ; journalisation (*logging*) systématique des accès	critères d'embauche plus stricts ; meilleur contrôle des activités quotidiennes du personnel ; formation continue du personnel ; audits spécialisés, systématiques et répétés de la sécurité	sécuriser les accès ; déterminer des zones internes d'accès restreint selon les besoins des tâches des employés ; suivi des déplacements des employés	partenariats avec les sites ou acteurs avoisinants ; améliorer la capacité de surveillance électronique ou humaine du site et des environs

Pallier aux défaillances de l'environnement physique se situe au niveau « tactique » de l'intervention immédiate. Trouver une solution adéquate à ce genre de problème sera efficace immédiatement et à court terme, mais la question de savoir combien de temps le problème restera réglé est ouverte. En effet, la plupart des solutions purement tactiques donnent lieu à des contre-solutions, constamment inventées par les individus décidés à continuer leurs activités dommageables. Par exemple, il n'est pas rare que la réduction d'un type d'activité à un endroit donne lieu à son apparition à un autre, phénomène appelé « déplacement ». Les approches purement tactiques peuvent aussi envenimer les relations sociales liant les personnes qui fréquentent les lieux.

Le second niveau de problème est celui des caractéristiques systémiques et institutionnelles. Ici, les *raisons* pour lesquelles des conduites dommageables sont adoptées par des personnes commencent à prendre de l'importance. On ne se demande plus si la clôture est suffisamment haute, mais bien, « *pourquoi* voudrait-on la franchir ? ». Par exemple, la prolifération de graffitis sur les murs d'édifices d'un quartier peut être conçue comme un problème purement tactique, nécessitant un meilleur éclairage des édifices ou l'installation de caméras pour décourager ou saisir les coupables. Elle peut aussi être conçue comme un problème systémique, par exemple l'absence de lieux ou d'installations où les jeunes peuvent adopter des activités alternatives moins irritantes pour les résidants du quartier (ou tout simplement une mauvaise synchronisation de la fin des classes et des moyens de transport des élèves). Identifier de telles activités, des lieux où elles peuvent se dérouler et les ressources humaines et financières nécessaires à leur création peut se révéler un casse-tête insoluble et n'est évidemment pas à la portée de tous. De plus, il n'existe pas de garantie que les graffitis disparaîtront immédiatement lorsque des avenues plus productives existeront. Rappelons tout de même que la prévention purement tactique n'est pas davantage garante de ses résultats.

Dans une organisation, les relations sociales entre les employés, les cadres, les « clients », les visiteurs et les membres d'autres organisations peuvent donner lieu à une impressionnante liste de « problèmes ». Il est évident que les conflits de travail entraîneront certaines conséquences facilement identifiables, telles que le vandalisme, le zèle inutile, la diminution de la productivité, etc. Cela dit, sans que les relations de travail se soient détériorées à ce point, une foule d'autres données relatives aux systèmes dans lesquels les individus doivent évoluer ont un effet sur leur conduite. Par exemple, Greenberg (1990) a montré comment les coupures dans les salaires font grimper les cas de vol au sein des entreprises ; à l'inverse, notons qu'une des raisons de l'augmentation fulgurante du salaire des policiers dans la deuxième moitié du 20^{e} siècle fut la nécessité de contrer leur corruption.

Enfin, placer un problème au niveau « social » c'est le placer à l'apex de la pyramide de la complexité. C'est le comprendre en le plaçant au centre d'un certain nombre de faits sociaux déterminants comme les grands courants

économiques, démographiques et idéologiques, les événements historiques, etc. qui façonnent non seulement les sociétés mais également les individus et les relations qu'ils entretiennent avec leur environnement.

Comme déjà mentionné, on pense souvent que ces éléments sont entièrement hors de portée de la plupart des entités aux prises avec des difficultés de sécurité — et qu'ainsi il est inutile d'identifier des problèmes « sociaux ». Ceci est évidemment faux lorsque le « client » de l'expertise en sécurité est un organisme gouvernemental qui vise justement à mettre sur pied un programme de prévention sociale de la criminalité, par exemple. En fait, la plupart des institutions gouvernementales, individuellement ou en tant que représentantes de l'État dans son ensemble, ont des missions se situant justement dans la sphère sociale (bien sûr, les points de vue politiques sont divisés sur l'étendue que devrait avoir le rôle de l'État en matière de programmes sociaux, d'intervention dans les relations sociales et de prestation de divers services).

Identifier un problème comme « social » peut également être utile pour d'autres types d'acteurs. L'entreprise qui perdait ses outils électriques identifia non pas un problème de sécurité, qui aurait amené une solution tactique, mais un problème de niveau social : la société de consommation exige qu'on achète les outils dont on veut se servir, même si c'est pour quelques heures par année, et ces outils sont généralement spécialisés, donc doivent être accumulés, à fort prix. La solution, dans ce cas, ne fut pas « sociale ». En effet, l'entreprise ne pouvait espérer changer la signification du concept de propriété dans notre culture, ou quelque autre notion du genre ! Il fut donc décidé de créer une « bibliothèque d'outils » que l'entreprise mettrait à la disposition de ses employés. Des fonds furent débloqués non pas pour ajouter des caméras ou des contrôles d'accès additionnels mais bien pour se procurer un grand nombre d'outils destinés à être tout bonnement prêtés aux employés qui décidaient de faire quelques rénovations chez eux un week-end. Cette solution, en plus de faire diminuer considérablement les vols, eut pour avantage de favoriser les bonnes relations de travail au sein de l'entreprise.

En fait, la plupart des organisations d'envergure moyenne et grande peuvent affecter la structure sociale, au moins localement. Elles peuvent financer des programmes de développement local, mettre certaines installations à la disponibilité du public pour des activités communautaires, contribuer à donner une apparence plus conviviale au quartier en modifiant l'aménagement extérieur de leurs édifices (dans la mesure où on considère l'aspect extérieur du quartier étant un facteur de son taux de criminalité, comme dans la théorie des « vitres cassées » ; Wilson et Kelling, 1982). Aucun de ces aspects ne produira des résultats immédiats, mais la sécurité ne doit pas uniquement être conçue à court terme.

Ici, il faut revenir un instant sur la place de la criminalisation des conduites indésirables dans les organisations, les quartiers, les édifices, les parcs, les écoles, etc. On aura remarqué l'absence des forces policières dans cet exposé. Comme mentionné plus haut, les lois pénales de la plupart des pays occidentaux permettent de confier à l'État la presque totalité des conduites représentant un problème réel de sécurité (ainsi qu'un ensemble infini d'autres qui n'en représentent aucun). Toutefois, même la police, et notamment dans les contextes de police dite « communautaire » ou « de proximité », évite souvent de traiter les problèmes comme des crimes, favorisant les solutions non pénales, qui sont souvent plus efficaces en termes de prévention (Brodeur, 2003). Étrangement, plusieurs manuels de sécurité, comme Fischer et Green (2004) débutent quand même leur section sur la planification de sécurité par une discussion de la nature de l'infraction criminelle et le fonctionnement du système pénal et présentant la sécurité privée interne comme une extension de la police et du système pénal.

Pourtant, en pratique il est difficile d'énoncer une règle ou principe permettant de juger à l'avance si un problème relève de la police, de la personne, organisme ou institution devant se protéger, ou des deux. D'ailleurs, la plupart des programmes de police communautaire incluent, du côté policier, l'établissement de partenariats avec les milieux et avec les personnes dont il faut assurer la sécurité, dans lesquels un certain nombre de situations sont définies comme étant de leur ressort. Il semble raisonnable, en tant qu'axiome de départ, de confier tous les crimes graves (par exemple, les vols de plus de 5 000$ et la violence causant des blessures physiques) aux forces de l'ordre. Pour le reste, l'appel à la police, que ce soit pour une intervention spécifique ou pour établir un projet conjoint de prévention, reste simplement un élément possible d'une solution éventuelle.

L'analyste policier, bien sûr, verra les choses d'un autre angle. S'il est là à analyser une situation, c'est que des citoyens, ses supérieurs ou la surveillance routinière des statistiques sur la criminalité ont déjà déterminé qu'une action policière était nécessaire. Comme l'analyste non-policier, il doit aussi se demander si la solution doit inclure des procédures judiciaires contre des personnes : ce ne doit pas être une conclusion automatique (sauf dans le cas de crimes graves bien sûr ; mais même dans ce cas les solutions devraient dépasser le simple appel au pénal). La police dite « de résolution de problèmes » n'est pas une activité qui consiste à découvrir le meilleur moyen d'appliquer les outils de la justice criminelle. Pour faire de la police de résolution de problèmes de manière efficace, il faut au départ comprendre qu'une foule de solutions non-pénales sont souvent plus efficaces en termes purs de sécurité, et qu'il n'est pas intrinsèquement immoral ou injuste de contourner l'appareil judiciaire. La majeure partie de la littérature scientifique et technique sur la police converge vers une conclusion de plus en plus inévitable, que la production de sécurité ne peut efficacement reposer exclusivement sur les solutions policières et l'usage du

système pénal.

Une mise en garde s'impose tout de même : le système pénal est équipé d'un nombre impressionnant de garanties juridiques, plus ou moins efficaces mais du moins explicites, qui sont sensées empêcher que des abus soient commis contre les citoyens accusés de méfaits. Ces garanties n'existent pas, ou du moins pas de manière systématisée et explicite, en matière de solutions « non pénales ».

En bref : ce qu'est un problème

Certains préceptes de base doivent être appliqués à la définition de tout problème.

A. Un problème de sécurité a pour source une conduite humaine observée ou imminente présentant certaines caractéristiques tangibles, dont principalement sa gravité et sa répétition. La **gravité** peut se mesurer par les coûts financiers, humains et sociaux qui sont ou seront engendrés par la conduite. Ces coûts doivent dépasser la simple irritation ou nuisance, si on veut éviter la multiplication inutile des « problèmes » (voir tableau 23-2). Bien sûr, mis à part le calcul des pertes financières (non seulement la valeur de remplacement ou de réparation des biens volés ou endommagés, mais l'augmentation des primes payées aux assureurs, la perte de productivité engendrée par la disparition du matériel ou par les travaux de rénovation, etc.), les autres formes de « coûts » sont hautement subjectives mais non moins importantes, comme la disparition du sentiment d'être en sécurité. Sa **récurrence** est également une facette importante. Ici, il faut tout de même mettre un bémol aux conclusions d'auteurs comme Clarke et Eck (2003) qui en font une condition *sine qua non* de l'existence d'un problème : selon eux, pas de problème sans répétition. À strictement parler, ceci exclue les *risques* et les problèmes futurs de sites en préparation, alors justement qu'on en est à planifier les systèmes de sécurité. Il faut donc parler de répétition « virtuelle », selon les données disponibles sur des sites comparables.

B. Un problème a des *causes*. Il n'est pas particulièrement utile de s'arrêter à « les êtres humains veulent des choses ; si les choses sont là, ils les prendront ». La théorie du choix rationnel prévoit exactement cela, mais ne nous explique pas pourquoi certaines personnes ne se saisissent pas d'opportunités qui sont pourtant alléchantes pour d'autres. Les causes qui doivent être identifiées doivent aussi se situer à la portée des acteurs qui seront chargés de la sécurité (tout en tenant compte du fait que cette portée est souvent beaucoup plus large qu'on le suppose, comme nous l'avons vu).

C. Il est peu utile de conceptualiser les problèmes comme des « crimes ». Que les conduites visées soient effectivement criminelles a son importance bien sûr, mais par définition, un « crime » n'est jamais qu'un événement, commis par une personne en un lieu et temps précis — tout ce qu'un problème, tel qu'entendu ici, n'est pas.

D. La résolution des problèmes passe par la connaissance des situations factuelles et des opinions des acteurs concernés — donc, par la collecte et surtout l'*analyse* d'informations. Disposer d'informations suffisantes est bien sûr important, mais presque secondaire au développement de la capacité de les analyser. Aucune information n'est jamais réellement complète, sans compter que plusieurs sont protégées par des règles, comme celles relatives à la protection de la vie privée, entre autres. Une analyse compétente maximise la valeur des informations disponibles, *en fonction d'un but*. L'analyse ne vise pas à élargir la culture personnelle d'individus curieux, mais la *solution* de *problèmes*. Cet aspect peut sembler tenir de la nuance, mais il est au contraire capital de le comprendre correctement. Analyser, ce n'est pas tâtonner à l'aveugle parmi une mer d'informations disponibles, c'est organiser l'information selon des objectifs.

E. Ainsi, un problème concerne des *personnes* : celles qui adoptent les conduites indésirables, celles qui les subissent, celles qui en font l'expérience indirecte (témoins, passants, voisins, usagers, etc.), celles qui ont la responsabilité d'assurer la sécurité des lieux, biens et personnes. Les problèmes identifiés ne sont pas des accidents, des phénomènes naturels ou des coïncidences, ils doivent être articulés clairement en fonction des acteurs qui y jouent un rôle, et qui auront, ou pourraient avoir un rôle à jouer dans leur solution.

3 L'identification de solutions : imagination et initiative

Allons-y tout de suite d'une affirmation à la fois évidente et controversée : l'identification de problèmes est indissociable de l'identification de solutions. Si j'en ai traité ici séparément, c'est uniquement pour simplifier la présentation. En réalité, problèmes et solutions, en pratique, sont des concepts qui se chevauchent au point d'être pratiquement semblables. J'ai déjà discuté de l'évidence du serrurier centré sur les portes mal fermées, de l'installateur de caméras qui voit partout autour de lui des endroits non surveillés et du colporteur de portails de sécurité préoccupé par les visiteurs dissimulant des armes sous leurs vêtements. Ceci est le côté « évident » de l'affirmation. On doit circonscrire ce problème en faisant appel à un expert indépendant et, par conséquent, tout expert en sécurité devrait être en mesure de faire une démonstration convaincante qu'il n'est pas en conflit d'intérêts.

Il est impossible de faire un inventaire de solutions. On peut bien sûr noter quelles sont les meilleures pratiques (*best practices*), les solutions déjà utilisées qui ont donné de bons résultats (comme le font succinctement Clarke et Eck, 2003, par exemple). Ceci est d'autant plus facile si on conçoit les problèmes à un niveau strictement tactique, puisque l'inventaire des solutions correspondantes est relativement limité. Pourtant, même dans ce cas, faire une telle liste comporte plusieurs inconvénients qui ont déjà été effleurés plus haut : premièrement, faire une liste de solutions tend à transformer l'expertise en sécurité en exercice d'application de recettes, ce qui lui enlève toute forme d'intérêt, sauf commercial. Deuxièmement, l'usage de listes et de « meilleures pratiques » réduit à néant l'approche novatrice de l'expert, son imagination et sa faculté de s'adapter aux besoins. Son travail, plutôt que de consister à identifier les particularités des endroits, personnes et organisations qu'il doit sécuriser, se bornera plutôt à les classer dans un nombre restreint de catégories afin d'en reconnaître le plus bas dénominateur commun — c'est la sécurité « moule à biscuits », faite rapidement mais souvent peu adaptée aux besoins. Troisièmement, ces listes sont établies et validées avec des outils scientifiques souvent puissants et fiables, mais qui ne peuvent que mesurer selon des standards donnés par des préférences humaines subjectives et souvent arbitraires et discutables. Se concentrer exclusivement sur les baisses immédiates de statistiques criminelles, même dans un modèle quasi-expérimental irréprochablement construit, c'est ignorer une foule d'autres bénéfices et coûts que peuvent engendrer les fameuses meilleures pratiques. Enfin, les listes de solutions sont trompeuses : elles donnent à penser qu'il est simple de régler un problème avec l'installation de dispositifs, la formation de personnel, etc. choses qui sont en elles-mêmes hautement complexes. Par exemple, et comme il a été démontré à maintes reprises (entre autres par Grandmaison et Tremblay, 1997), la solution à la mode d' installer des caméras de surveillance occulte le fait incontournable qu'une installation moins qu'optimale de ces caméras ne donnera *jamais* les résultats escomptés.

Ainsi, ce chapitre ne comporte pas de liste de solutions à sélectionner et/ou adapter à l'infinie variété des problèmes passés, présents et futurs qui peuvent se présenter (le tableau 23-4 en donne tout de même une illustration). Cette section donne plutôt un certain nombre de principes de base qui doivent guider la recherche de solutions.

A. Aucune solution n'est parfaite, ni ne devrait viser la perfection. Ceci a comme corollaire qu'il faut prévoir une *réponse* aux incidents qui pourraient survenir malgré la présence de nos dispositifs de sécurité. Par exemple, il n'est pas réaliste de croire qu'on puisse se protéger du terrorisme chimique dans nos moyens de transport en commun. Cependant, il ne faudrait pas conclure à ceci qu'il n'y a rien à faire : il est impératif, au contraire, d'avoir un plan de secours (*contingency plan*), et mettre sur pied des moyens de limiter les dégâts et de permettre aux activités normales de se poursuivre aussitôt que possible.

B. Il faut tenir compte des effets négatifs inhérents à toute intervention visant l'amélioration de la sécurité. Si une solution donnée n'a aucun effet négatif immédiatement apparent, c'est probablement qu'on a mal analysé la situation. La plupart des ouvrages de prévention situationnelle, qui consiste à réduire et à contrôler les opportunités d'adopter une conduite dommageable, présentent les solutions comme de simples modifications environnementales, et donc avec pour seul aspect négatif les déboursés financiers engendrés par ces modifications. Ceci est d'une myopie dangereuse. Toutes ces solutions ont des impacts sociaux et organisationnels négatifs qu'il est impératif de minimiser — pour se faire, il faut d'abord les reconnaître et les accepter.

C. Il faut déterminer la nécessité d'intervenir : la première étape de toute recherche d'une solution est de déterminer la gravité réelle des faits et des conduites identifiées, à commencer par déterminer s'il y a réellement problème ou non, au sens où on l'entend ici. S'il s'agit de *crimes*, en termes purement légaux leur gravité est relativement facile à évaluer : la loi prévoit déjà une échelle de gravité des actes commis. Seulement, ceci est peu pratique en réalité. Non pas qu'il faille contrevenir à la loi, mais bien que la loi, étant par définition générale, s'applique à une multitude de cas sans les différencier. Selon la loi, le moindre graffiti peut constituer une infraction pénale. De même pour les altercations mineures, les vols sans importance et autres « incivilités ». Dans la plupart des cas ces conduites ne sont pas des *problèmes* et il est inutile de leur trouver une solution. Définir le moindre irritant de la vie quotidienne en termes de « problème » est peu productif, engendrera des coûts prohibitifs et détournera l'attention des failles plus graves. Toutefois, dans la mesure où ces conduites deviennent répétitives, endémiques, qu'elles ont un impact significatif sur la qualité de vie des personnes, elle peuvent effectivement devenir des problèmes (bien qu'elles aient été des infractions pénales depuis le début).

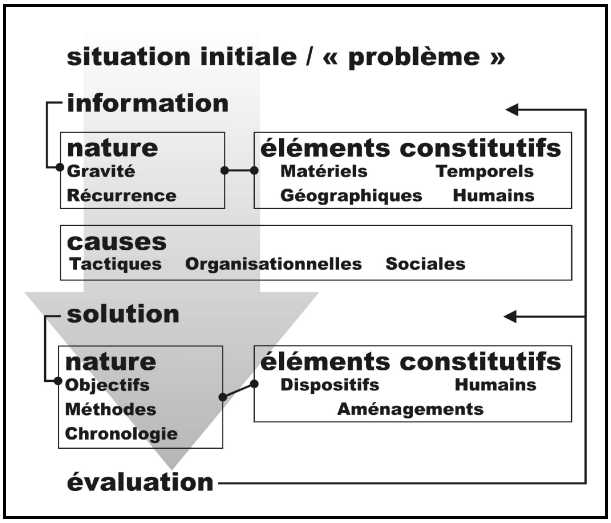
D. Ceci peut paraître évident, mais il faut tout de même souligner que toute solution doit avoir pour objectif de réduire le problème identifié. Il est commun pour les praticiens de prendre le déploiement des méthodes, des techniques et des technologies visant la résolution du problème pour un *objectif* — autrement dit, le succès du déploiement de la solution est considéré comme le succès de la solution. Par exemple, l'installation rapide et efficace d'un système de contrôle d'accès ou l'affectation de patrouilles policières additionnelles constituerait déjà un *succès*. Ceci est une erreur assez grave. Le déploiement de la solution doit être couronné

de succès, bien sûr, mais ce n'est qu'une étape intermédiaire vers le but visé, qui est de réduire l'ampleur du problème. Il est important d'identifier des objectifs clairs et mesurables (ce qui ne signifie pas nécessairement au sens statistique du terme) ; ces objectifs doivent posséder 4 facettes : 1) chronologie : on doit énoncer clairement le début de l'action proposée et le moment où on s'attend à des résultats. 2) Qui est impliqué : ici, il s'agit de mettre à profit les caractéristiques, capacités et intérêts de tous les acteurs touchés par le problème, et d'énoncer clairement quel devrait être leur rôle et comment on s'y prendra pour les mobiliser. 3) Où se déroulera l'activité : ceci est relativement évident lorsqu'un site particulier est visé, mais beaucoup moins dans le cas de problèmes liés à l'échange d'information. Dans ces cas, la question de l'espace peut devenir un écheveau inextricable. 4) Un énoncé clair de l'effet qu'on veut produire.

E. On l'oublie souvent, mais il faut que la solution proposée ait une chance raisonnable, sur papier, d'atteindre l'objectif visé. Ceci 1) évitera de lancer n'importe quoi au problème en se croisant les doigts ; 2) permettra de comparer les coûts du problème aux coûts de la solution (qui incluront une partie restante, irréductible du problème).

F. Toute activité organisée visant à améliorer la sécurité doit *évaluer* ses résultats. Plusieurs méthodes de mesure systématiques sont disponibles, dont bien sûr la comparaison avant/après, avec ou sans site contrôle (ce qui veut dire, bien sûr, qu'il faut avoir prévu cette évaluation des résultats *avant* de mettre en place la solution préconisée). Il n'est pas exclu d'évaluer une solution à l'aide de méthodes qualitatives, sauf si on confond « qualitatif » avec « bâclé », comme c'est souvent le cas. Une évaluation qualitative doit être faite avec rigueur et ne consiste pas, par exemple, à recueillir ici et là l'opinion de certaines personnes importantes, ou qui étaient disponibles ce jour là. Une évaluation bâclée n'est pas *moins valable* qu'une bonne évaluation : elle est carrément *inutile*, sa valeur est de zéro. Ainsi, multiplier les méthodes approximatives d'évaluation ne mène nulle part.

Figure 1 : processus de résolution de problèmes



Conclusion

Le processus de résolution d'un problème de sécurité est, on le voit, à la fois relativement linéaire, simple à suivre et hautement complexe dans les détails de la démarche. Il demande également un esprit formé non pas à l'application de solutions mais bien à la découverte de possibilités adaptées aux spécificités de chaque situation.

Comme le montre la figure 1, cette linéarité du processus inclue tout de même certaines boucles de rétroaction où la pratique, la mise en place de solutions et l'observation de leurs effets, viennent modifier la connaissance qu'ont les acteurs de la situation. Souvent, les évaluations initiales, même lorsqu'elles sont menées de manière irréprochable, restent perfectibles. De toute manière, les situations humaines sont fluides et en constante évolution et il ne faut pas s'attendre à ce qu'une solution efficace le soit à jamais. Ainsi, une collecte constante d'information sur les pratiques et sur leurs effets peut s'avérer particulièrement fructueuse.

Références

Broder, James (2000), *Risk Analysis and the Security Survey, Second Edition*, Boston, Butterworths Heinemann.

Brodeur, Jean-Paul (2003), *Les visages de la police*, Montréal, Presses de l'Université de Montréal.

Clarke, Ronald et John Eck (2003), *Become a Problem-Solving Crime Analyst in 55 Small Steps*, Londres, Willan.

Cohen, Lawrence et Marcus Felson (1979), « Social Change and Crime Rates », *American Sociological Review*, N°44, 588-608.

Cope, Nina (2003), « Crime Analysis : Principles and Practice », T. Newburn, *Handbook of Policing*, 340-362.

Ericson, Richard et Aaron Doyle (2004), *Uncertain Business: Risk, Insurance and the Limits of Knowledge* Toronto, University of Toronto Press.

Fischer, Robert et Gion Green (2004), *Introduction to Security*, Boston, Elsevier.

Grandmaison, Rachel et Pierre Tremblay (1997), « Évaluation des effets de la télé-surveillance 93-110.

Greenberg, Jerald (1990), « Employee Theft as a Reaction to Underpayment Inequity : the Hidden Costs of Pay Cuts *», Journal of Applied Psychology*, 75 (5), 561-568.

Johnson, Brian (2005), *Principles of Security Management*, Upper Saddle River (New Jersey), Pearson Prentice Hall.
Shearing, Clifford (2000), « Punishment and the Changing Face of Governance », *Punishment and Society*, 3 (2), 203-220.
Toch, Hans and J. Douglas Grant (2005), *Police as Problem Solvers, 2nd Édition*, Washington, American Psychological Association.
Trojanowicz, Robert et Bonnie Bucqueroux (1998), *Community Policing : How to get Started, 2nd Edition*, Cincinnati, Reading.
Willis, James, Stephen Mastrofki et David Weisburd (2003), *Compstat in Practice : An In-Depth Analysis of Three Cities*, Washington, Police Foundation, http://www.policefoundation.org/pdf/compstatinpractice.pdf.
Wilson, James et George Kelling (1982), « Broken Windows », *The Atlantic Monthly*, 249 (3), 29-38.