Les nouvelles technologies de l'information et leur impact sur la sécurité... : Les défis de la recherche scientifique en Suisse

Autor(en): **Ribaux, Olivier**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **144 (1999)**

Heft 9

PDF erstellt am: **09.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-348731

Les nouvelles technologies de l'information et leur impact sur la sécurité...

Les défis de la recherche scientifique en Suisse

La délinquance a évolué rapidement, en particulier en raison du développement des moyens de transport et des réseaux de communication. Les activités criminelles mettent en jeu beaucoup de personnes et d'objets organisés dans des structures complexes et coordonnées. Certaines utilisent de manière efficace les nouvelles technologies de l'information.

Olivier Ribaux[1]

Le marché de la drogue et le crime informatique sont des exemples de ces formes de criminalité, aujourd'hui si difficiles à identifier, à cerner et à interpréter dans l'ensemble des informations accessibles et sous les contraintes d'ordre juridique et économiques auxquelles la police doit faire face. Ce n'est que lors de la découverte d'affaires importantes qu'on se rend compte de l'ampleur des activités mises à jour et du danger pour la sécurité publique qu'elles représentent, déjà en temps de paix. Dans une situation de conflit, ces risques se multiplient: désorganisation de l'Etat et atteintes à l'économie peuvent, par exemple, résulter d'une exploitation malveillante de l'information.

De nouvelles stratégies d'investigation et de gestion de l'information sont nécessaires. Leur définition et leur intégration dans la pratique constituent des défis pour la recherche scientifique appliquée aux mondes de la police, de la justice et de l'armée. La maîtrise et l'interprétation des informations ne sont toutefois pas suffisantes. Elles servent principalement à comprendre les menaces, les stratégies adverses et ainsi à orienter la mise en œuvre d'actions appropriées bien coordonnées. La transformation de ces informations en mesures concrètes est un autre axe primordial à explorer.

Problématique: l'exemple Internet

Pour illustrer ces risques et se convaincre de l'ampleur des questions soulevées, quelques heures passées devant un ordinateur à «surfer» sur Internet suffisent. Une grande variété d'infractions se produisent indépendamment des frontières, sans notion de distance, au travers de systèmes juridiques souvent peu compatibles et hermétiques; leur impact sur la sécurité publique est encore loin d'être mesuré.

Accès aux sites pornographiques

Les sites pornographiques de tous les genres, accessibles en particulier aux plus jeunes très à l'aise dans ce monde virtuel, ne constituent qu'une facette de la question.

Accès à des recettes pour commettre des actions criminelles ou échapper à la justice

La diffusion de recettes pour commettre des crimes et délits en tous genres, de l'utilisation frauduleuse de cartes de crédits à la fabrication d'explosifs, en passant par les moyens les plus avancés de produire des drogues, incite sans doute au passage à l'acte. Cette information, certes autrefois accessible, mais au prix d'efforts considérables, est aujourd'hui visible de n'importe quel point

[1] *L'auteur partage son temps entre la Police vaudoise et l'Institut de police scientifique et de criminologie à l'Université de Lausanne. En 1996, la Conférence des commandants des polices cantonales de Suisse romande a estimé nécessaire d'engager un spécialiste universitaire pour renforcer la structure de coordination judiciaire développée entre ses membres et renforcer l'analyse scientifique des renseignements.*

Institut de police scientifique et de criminologie, Université de Lausanne, CH, 1015 Lausanne-Dorigny (tel. +41 21 692 46 00; fax: + 41 21 692 46 05; e-mail: Olivier.Ribaux@ipsc.unil.ch).

de la planète, et obtenue immédiatement au moyen d'outils de recherche simples et efficaces.

Désinformation

La diffusion d'informations comme l'incitation à la haine raciale, la publicité pour certaines sectes ou toute autre forme d'informations déformées et dont la source est difficile à contrôler sont susceptibles de causer des dégâts considérables.

Contrefaçon

Copies de programmes, possibilité de construire ses propres CD musicaux à partir d'informations trouvées sur le réseau: la propriété intellectuelle est également en danger.

Accès facilité à des prestations

Les casinos virtuels ruinent les plus vulnérables, comme le font d'autres prestations accessibles au moyen d'une carte de crédit. De plus, les possibilités sont nombreuses d'accéder à des services en usurpant l'identité de victimes.

Les programmes utilisés comme des armes

Souvent, cette information ne circule souvent pas en sécurité et subit des attaques permanentes par une grande variété de programmes dont les virus informatiques constituent la famille principale.

Accès à des données ou à des prestations

Accéder à des données sensibles semble constituer un défi intellectuel auquel des inconscients résistent avec peine. La perception de commettre un

La police doit disposer de moyens qui lui permettent de lutter avec efficacité contre la criminalité...

délit est faible, voire inexistante, car il n'existe aucune véritable stratégie de prévention; au contraire la société semble parfois encourager ces pratiques en élevant le «pirate informatique» au rang de «petit génie». Certes, le malfaiteur ne procède par aucune violence physique, et les dégâts occasionnés sont abstraits; mais les conséquences indirectes sont parfois dramatiques. Face à la complexité des réseaux, la mise en place de systèmes de sécurité, bien que théoriquement possible, n'est pas aisée d'un point de vue pratique: le nombre de paramètres à gérer est considérable et leur influence mutuelle a souvent des conséquences inattendues qui ouvrent des accès aux délinquants.

L'accès aux données est également favorisé par la naïveté des utilisateurs: les mots de passe sont souvent prélevés et révélés par une grande diversité de programmes. Le statut de «génie» du pirate informatique n'est donc de loin pas mérité. Beaucoup de patience, de persévérance, de débrouillardise et de bons outils suffisent parfois à pénétrer dans les centres les plus réputés. Si le petit délinquant parvient déjà à causer de grands dégâts, la menace devient sérieuse lorsque des organisations «professionnelles» procèdent avec systématique.

Autres menaces

Cet inventaire est très général et pas exhaustif; pourtant, Internet ne constitue qu'une partie du problème. L'espionnage économique et militaire, le détournement de transactions, les délits d'initiés par l'accès à des données secrètes, etc. sont des activités basées strictement sur l'exploitation de faiblesses dans les systèmes

d'information; elles sont susceptibles de déstabiliser, voire de conduire les victimes à la ruine.

Les nouvelles technologies sont également largement utilisées par le crime organisé international, qui les exploitent pour coordonner et planifier ses actions. Par exemple, le téléphone portable, volé ou dont les numéros changent sans cesse grâce à des cartes interchangeables, est un outil privilégié des trafiquants de stupéfiants. Toute action internationale et organisée passe par l'utilisation des nouveaux moyens de communications.

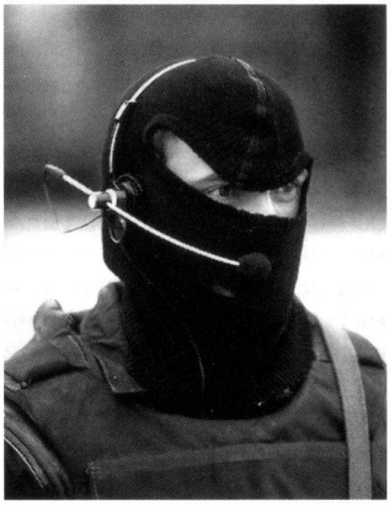
Décalages dans les moyens de lutte

La police utilise ces nouvelles technologies comme arme contre la criminalité. Toutefois, elle effectue ce travail en ne pouvant bénéficier que d'une recherche limitée et dans des conditions difficiles.

On peut par exemple s'intéresser à un problème grand par le nombre de cas, mais qu'on pense généralement bien maîtrisé: le cambriolage. Quelle est l'ampleur du problème? Quelle est l'évolution au cours des derniers mois en Suisse? Impossible de le savoir car aucune base de données centralisée ne contient ces informations actualisées pour l'ensemble de la Suisse. Des statistiques annuelles paraissent... avec trois mois de retard. Des données sont certes accessibles, mais généralement distribuées à travers tout le pays. De plus, la manière dont les informations sont récoltées et la signification des notions utilisées varient d'un canton à l'autre et empêchent de se faire une idée objective du phénomène.

Jusqu'à la création de structures plus performantes dans les organisations de police et de travaux de recherches dans le domaine, aucun «tableau de bord» de ce phénomène n'était disponible pour un problème considéré pourtant souvent comme «simple» et «anodin». Les conditions ne sont donc pas favorables pour aborder les questions plus difficiles.

A priori, le contraste avec la manière dont l'information est couramment traitée dans d'autres domaines est frappant: par exemple, la bourse est maintenant électronique et les cours sont largement disponibles en «temps réel» pour tous ceux qui disposent d'un matériel minimum. Il n'est plus possible d'effectuer des achats dans les magasins sans que, grâce à des techniques pointues d'exploitation des données appelées «data mining», des bases de données ne soient exploitées pour construire les profils des clients; ces descriptions servent ensuite à cibler la publicité, à disposer les marchandises dans les rayons, etc. La guerre économique fait tellement rage qu'il s'agit de se renseigner sur l'état de santé et les projets de ses concurrents; ainsi, une nouvelle discipline strictement basée sur la récolte et le traitement du renseignement sur les entreprises, appelée en anglais «competitive intelligence», se développe en Europe et en Suisse, par l'intermédiaire de sociétés de services. Enfin, dans un domaine connexe au travail de la police, de grands consultants construisent et utilisent des outils statistiques d'investigation en matière économique. Ce type d'investigation échappe au domaine de compétence de l'Etat.



Dans les groupes d'intervention, il faut communiquer en temps réel.

On pourrait citer beaucoup d'autres exemples dans lesquels des principes, des méthodes et des techniques seraient adaptables, à des degrés et des niveaux divers, au domaine de l'investigation criminelle. Les raisons de ce décalage entre la manière dont la police peut gérer ses informations et l'explosion des possibilités technologiques sont multiples. Les lois qui régissent les projets ayant une composante informatique constituent un frein considérable pour les développements et empêchent l'utilisation efficace de l'information. En effet, à la suite de l'«affaire des fiches», les craintes liées à l'utilisation de renseignements par le système judiciaire ont renforcé les règles. L'applica-

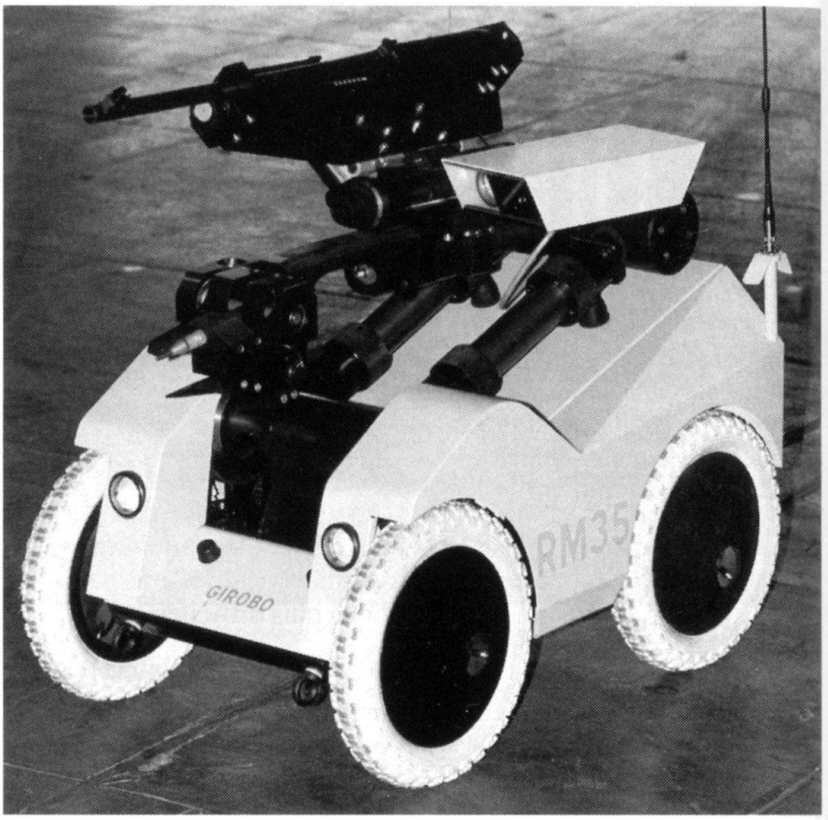
tion sous une forme automatisée de méthodes d'investigation pourtant courantes est souvent interdite pour le plus grand profit des criminels.

L'essentiel du problème ne réside donc pas dans l'informatique elle-même, mais plutôt dans les méthodes utilisées. Une information récoltée avec des buts bien définis, dans un cadre structuré et aussi bien formalisé que possible, est sans doute la meilleure garantie pour le citoyen et sa sphère privée; une informatisation découlant de ces réflexions conduirait nécessairement à une gestion solide du renseignement, qui rassurerait sur les risques de dérapages.

Toutefois, les questions sont beaucoup plus difficiles qu'on ne pourrait le penser a priori; l'investigation des différents types de crimes est souvent spécifique et complexe. La conception de modèles particuliers pour gérer les affaires criminelles, la création de compétences dans ces domaines sont nécessaires.

Réactions

Face à ces faiblesses, il serait faux de prétendre que l'Etat ne réagit pas. De nouvelles structures, à l'échelle de la Confédération et des cantons, favorisent l'échange et le traitement de l'information entre les polices. Ces expériences jouent le rôle de «prototypes», de concrétisation à l'échelle réduite de la forme que pourrait prendre des structures plus ambitieuses. Elles posent également,



Un «robot» pour les forces de police.

dans la pratique, de nouvelles questions qu'il n'était pas possible d'anticiper, dans une démarche itérative très appropriée à la complexité des questions traitées.

Des méthodes d'analyse criminelle, expérimentées avec succès également en milieu militaire, permettent de structurer et d'uniformiser le traitement de l'information; des systèmes informatisés aident à l'application de ces méthodes; ils permettent notamment de visualiser des phénomènes complexes et favorisent ainsi l'exploitation objective et efficace du renseignement.

Les premiers «cyberpoliciers» suisses, chargés de traiter les questions liées à Internet sont aujourd'hui actifs. Bien que proportionnellement largement moins nombreux que leurs collègues des pays limitrophes, ils obtiennent des premiers résultats encourageants. Quelques juges, policiers et chercheurs échangent leurs connaissances et leurs expériences dans ce domaine, contribuant ainsi à élever le niveau de compétence dans l'ensemble du système. Les premiers pas sont effectués, mais les moyens investis et les outils à disposition restent insuffisants.

Le monde politique, le personnel de la police, les chercheurs et la presse relaient assez largement ces inquiétudes. De nombreuses réflexions sont menées pour adapter les structures, évaluer les conséquences

des contraintes légales sur le traitement de l'information, redéfinir les tâches et les rôles dans notre système fédéraliste, définir des programmes de formation orientés principalement vers le traitement du crime organisé.

Quelle sorte de recherche?

Ainsi, les retards ne résultent certainement pas d'un manque d'intérêt ou de l'absence d'engagement des professionnels; les faiblesses essentielles résident dans un manque d'activité de recherche dans ces domaines, doublé d'un excès de contraintes.

La complexité des questions soulevées nécessite une recherche spécifique intense de nature pluridisciplinaire. On peut schématiquement dire que des moyens techniques et des méthodes sont exploités par des policiers, dans des organisations, sous toute une variété de contraintes, essentiellement légales et économiques, tout cela dans un cadre donné par la politique criminelle. Les solutions doivent ainsi provenir de milieux très différents, s'imbriquer de manière à construire une architecture cohérente qui intègre les différents composants. Amener entre autres des policiers, des militaires, des managers, des politiciens, des juristes, des sociologues, des psychologues, des criminologues, des scientifiques et des économistes à communiquer leur point de vue est un défi à relever. Les difficultés spécifiques et les contraintes nécessairement imposées aux partenaires doivent être traduites dans un langage compréhensible, tout en donnant à ces différentes disciplines leur poids respectif approprié.

L'Université et la recherche peuvent largement contribuer à des rencontres, des réflexions, au développement de solutions directement applicables à la pratique. A l'étranger, des moyens existent déjà, mais leur adaptation à nos structures et à notre échelle, ainsi que leur intégration dans la pratique nécessitent des études approfondies. En Suisse, de nombreux chercheurs disposent des connaissances nécessaires pour aborder ces questions, et travaillent même dans des domaines plus ou moins directement connexes. Cependant, ils sont trop souvent éloignés de la pratique et n'ont pas l'occasion de situer l'efficacité de leurs travaux dans leur contexte réel.

Essentiellement à cause de l'aspect sensible des données et de la nécessité d'entretenir une certaine discrétion autour des méthodes utilisées, le relais entre la recherche et la pratique doit se réaliser dans le cadre d'un nombre restreint de structures de confiance. Plusieurs d'entre elles existent et ont déjà une longue expérience; il n'est donc pas nécessaire d'en créer de nouvelles, qui amèneraient beaucoup de redondance et qui rendraient l'ensemble du système difficilement contrôlable. Il s'agit plutôt d'étendre le champ de compétence de celles qui existent et de structurer les interfaces avec la pratique.

C'est d'ailleurs un thème proposé au Fonds national suisse de la recherche scientifique (FNSRS): créer un pôle national de recherche en Suisse orienté sur ces sujets. Il convient toutefois de souligner que, parmi les quelque deux cents projets présentés, moins d'une dizaine seront retenus!

Conclusion

Il faut souhaiter que l'ampleur des questions posées amèneront à faire admettre l'importance stratégique de projets qui visent à comprendre, à maîtriser et à exploiter les technologies de l'information, dans le but de maintenir la sécurité. Pourtant, l'objectif d'une structure sécuritaire saine et performante ne semble que peu préoccuper les milieux susceptibles de soutenir la recherche. Il ne s'agit pas toujours d'affronter directement une violence physique, facilement visible, mais de lutter dans le monde abstrait de l'information; les conséquences sont indirectes, donc difficiles à mettre en évidence a priori. Cela laisse peu de chance à des financements visant une recherche de pointe dans ce domaine.

O. R.