

Cours 11 : le renseignement, l'information, le risque

L'organisation du renseignement criminel et de sécurité au Canada ; les buts du renseignement ; la police du savoir ; la gestion des risques.

- a. Nouveau modèle policier : la « **police de renseignement criminel** » (*intelligence-led policing*) (texte de Dupont, 2002)
 - i. Fondée sur le concept de *risque* : non pas qu'il y a davantage ou moins de risque qu'auparavant, mais bien qu'un calcul « actuariel » des probabilités qu'un événement arrive ou non doit gouverner la prise de décision stratégique.
 - ii. Exemple : profilage criminel, prévention stratégique
 - iii. L'élément de base de cette conception est donc l'information : pour évaluer les risques, il est impératif de disposer de l'information nécessaire. Dans la sphère de la police, il s'agit de *renseignement policier* et de *renseignement de sécurité*.
 - iv. C'est une nouvelle conception de la criminalité, non pas sous forme d'incidents, mais bien de probabilités influencées par la qualité de l'information disponible.
 - v. Conséquences :
 - (1) multiplication des collectes de données et des banques de données sur tous les aspects de la vie
 - (2) répartition du travail selon les « points chauds »
 - (3) surveillance accrue de personnes « à risque »
 - (4) recentralisation du pouvoir policier, utilisation à distance des agents de police, retrait de l'expérience-terrain
 - (5) relative inutilité des relations communautaires

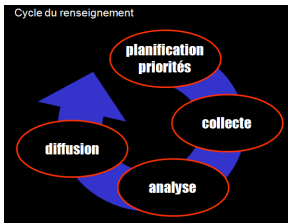
PPT

- b. Nature du renseignement
 - i. **Définition** : le renseignement, c'est l'organisation logique, utile, efficace d'une suite d'informations portant sur un sujet particulier.
 - (1) renseignement *criminel* : porte sur les auteurs, les événements, les sentences, les réseaux, les actifs et passifs, les déplacements, les endroits, les moyens de transport, les méthodes de communication, etc. **relatifs au crime commun**.
 - (2) renseignement de *sécurité* : porte sur la prévention des attaques contre la sécurité nationale (subversion, ingérence de puissances étrangères, espionnage, terrorisme). Le renseignement de sécurité **s'étend à l'étranger**.
 - (3) renseignement *militaire* : porte sur l'équipement, les effectifs, les déplacements, les méthodes, les technologies, les stratégies et tactiques de forces militaires étrangères. Inclue la protection des bases des forces canadiennes (FC).
 - (4) *le renseignement ne constitue pas une preuve*. La preuve est de nature différente, elle vise l'inculpation d'individus, et doit répondre à des critères légaux stricts. Ainsi, *savoir* n'est pas équivalent à *pouvoir prouver*.
 - ii. Sources de renseignement :
 - (1) sources « ouvertes » : en général, correspond à ce qui est disponible au public : médias, documents officiels, publications, discours publics, procès, rapports d'expertise, Internet(...), rapports annuels
 - (2) sources « fermées » : ce qui est *confidentiel*, réservé, d'usage exclusif, ou « secret défense » : infiltration, délation, observation directe, interceptions, surveillance, échanges, analyse avec « plus-value ».
 - iii. Types de sources
 - (1) HUMINT : (Human Intelligence). Correspond à l'ensemble des sources humaines, témoignages, infiltration, observation, interrogatoires, délation, écoute directe.
 - (2) SIGINT : (Signal Intelligence). Ici on regroupe les interceptions diverses de communications, et par extension les sources impliquant une forme de technologie de surveillance.

- (3) Documents : il existe généralement une montagne de documents sur les sujets qui peuvent intéresser un organisme de renseignement. Les difficultés sont de i. savoir qu'ils existent; ii. les trouver, iii. savoir être sélectif.

c. Cycle du renseignement

- i. Planification / identification d'objectifs : au départ, les autorités politiques ou administrative établissent des priorités



- ii. Collecte : étape où on amasse les informations. Il faut veiller à leur validité en les corroborant si nécessaire.
- iii. Analyse : étape la plus importante. On pense souvent au renseignement en termes de collecte, et on cherche toujours à amasser davantage. Ceci est une erreur : inutile de collecter plus d'information qu'on est capable de digérer. L'analyse donne de la valeur à l'information brute en la rendant intelligible. Elle permet la formulation de certaines hypothèses sur ce qui se passe, qui connaît qui, qui fait partie ou ne fait pas partie d'un réseau, etc.

- iv. Diffusion : à ce stade il faut remettre à ceux qui en ont besoin le résultat des analyses. Cette diffusion aux « clients » engendre un nouveau cycle, de nouvelles cibles et missions.

- v. Problème : *partage de l'information*. Toutes les organisations subissent une certaine tension entre la nécessité pratique, dans un but collectif, de mettre en commun le renseignement, et la volonté de d'individus de conserver pour eux des informations précieuses.

d. Buts du renseignement

- i. Objectifs **tactiques** : renseignements nominatifs visant la conduite d'enquêtes

- (1) réseaux de criminels
- (2) activités illégales
- (3) modus operandi
- (4) capacités, limites, intentions de groupes / d'individus
- (5) sources de financement
- (6) individus / groupes subversifs
- (7) espions (militaires, industriels etc)

- ii. Objectifs **stratégiques** : renseignements servant à orienter les priorités, politiques et pratiques policières ou gouvernementales

- (1) état de situation
- (2) tendances à long terme
- (3) évolution du milieu criminel
- (4) identification / évaluation de menaces à l'ordre public
- (5) transformation du cadre normatif
- (6) programmes de contre-offensive
- (7) modification des politiques criminelles ou des relations diplomatiques

e. Organismes de renseignement

- i. Renseignement **criminel**

(1) **GRC**

- (a) dans les années 1970 le renseignement criminel reste une activité ad hoc: on en fait lorsqu'on en a besoin (grandes enduites, événements)
- (b) à partir de 1980 le renseignement, en tant qu'activité permanente, continue, prend son envol avec le Fichier des crimes graves (FCG), avec lequel on tente de conserver la trace de différentes informations relatives à des crimes contre la personne. Remplacé par le Système d'analyse des liens sur la violence associée aux crimes (SALVAC).
- (c) niveau **interne** : Direction du renseignement criminel ; outil : Banque nationale de données criminelles (**BND**)
- (d) niveau **national** : **Service canadien du renseignement criminel** (SCRC).
 - (i) le SCRC est un centre d'intégration du renseignement policier national.

- (ii) ce renseignement est ensuite diffusé par le biais du **SARC**, Système automatisé de renseignements sur la criminalité (380 organismes-membres ont accès) (*Automated Criminal Intelligence Information System* (ACIIS))
 - (iii) **CIPC** (Centre d'information de la police canadienne) contient les descriptions de biens et voitures volés, et accès à d'autres banques de données
- (2) Québec
- (a) Depuis 2001, Service du renseignement criminel du Québec (**SRCCQ**). Le SRCQ fait pour l'essentiel la gestion et la rediffusion du renseignement entre les corps policiers du Québec et la GRC (faisait auparavant partie du SCRC).
 - (b) Est formé de personnel « prêté » par les corps de police (SQ et SPVM, surtout)
 - (c) Fait également certaines analyses, surtout de criminalité organisée et de traffics (alcool, tabac, .

ii. Renseignement de **sécurité**

- (1) **SCRS** (Service canadien de renseignement de sécurité) est une agence civile sous la responsabilité du ministère de la Sécurité publique et de la Protection civile (ministre : Stockwell Day)
- (a) contre-espionnage
 - (b) terrorisme
 - (c) filtrage de sécurité
 - (d) influences/ingérences étrangères
 - (e) le SCRS est une agence civile spécialement créée en 1984 après que plusieurs scandales aient éclaté au sujet des activités de sécurité de la GRC.
 - (f) ceci veut dire que les agents du SCRS n'ont pas le statut d'« agent de la paix » dont disposent les policiers. Lorsqu'ils constatent qu'un crime a été ou sera commis ils doivent se référer à la GRC, qui est l'organisme responsable.
 - (g) les activités du SCRS à l'étranger se limitent
 - (i) servir de liaison avec des services de renseignement étrangers (24 pays)
 - (ii) produire des compléments d'enquête dont les sujets sont au Canada.
 - (h) le SCRS est un partenaire clé des Équipes intégrées de la sécurité nationale (EISN), sous l'égide de la GRC.
 - (i) Un Comité de surveillance des activités de renseignement de sécurité veille à assurer que les agents du SCRS respectent les lois.
- (2) **CST** (Centre de la sécurité des télécommunications)
- (a) est une agence *militaire* sous l'égide du ministère de la Défense nationale (MDN) et des Forces canadiennes (FC) (ministre : Gordon O'Connor)
 - (b) Créée en 1947, sous l'accord UKUSA, entre les ÉU, le Canada, l'Australie et le Royaume Uni. L'accord vise principalement à l'interception des communications du bloc soviétique.
 - (c) les activités du CST sont en principe réservées à l'étranger, mais s'étendent au Canada dans certaines exceptions.
 - (d) fonctions principales
 - (i) cryptologie
 - (ii) sécurité informatique
 - (iii) interception
 - (e) Aucune loi du CST n'existait avant décembre 2001 et la *Loi antiterroriste*, qui contenait une section au sujet des fonctions et cadre réglementaire du CST
 - (f) Un Commissaire du CST surveille les activités de l'organisme. Le dernier en poste, l'ex-juge en chef de la Cour suprême du Canada, Antonio Lamer, jugeait que le cadre législatif du CST était trop flexible.
 - (g) Le CST doit maintenant « fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité »