Espionnage/Contre-espionnage
SOMMAIRE

INTRODUCTION

Une centaine d'années avant notre ère chrétienne, le stratège et philosophe chinois Sun Tse écrivait : "Ayez des espions partout, soyez instruits de tout, ne négligez rien de ce que vous pourrez apprendre… Une armée sans agents secrets est un homme sans yeux ni oreilles".
Rien n'a changé aujourd'hui et, pour éviter le triste sort dépeint par Sun Tse, celui d'être coupé de l'extérieur ou d'être pénétré, **espionnage et contre-espionnage** sont toujours indispensables, non seulement aux armées, mais aussi aux Etats dans la réalisation générale de leur politique.

Dans le renseignement moderne, on distingue quatre métiers.
Tout d'abord **l'acquisition** du renseignement, qui consiste à obtenir des informations spécifiques provenant de régions du monde "ouvertes" ou "fermées" en utilisant des moyens à la fois humains et techniques;
Vient ensuite la **réalisation d'analyses et de synthèses** qui consiste à traiter toutes les informations rassemblées en vue de remettre aux décideurs politiques un produit fini plus cohérent et plus intelligible que les données brutes;
Puis nous avons la **mission de protection**, qui comprend l'identification ainsi que la manipulation et la neutralisation éventuelles d'entités hostiles à la communauté nationale.
Enfin vient **l'exploitation, ou action**, qui est l'aboutissement, si besoin est des trois tâches précédemment définies et qui consiste à influencer, sans révéler son propre engagement, des Etats, des forces politiques, économiques ou sociales, ou encore à infléchir des événements dans le sens voulu par le pouvoir politique.
Espionnage et contre-espionnage, qui ne sont que des aspects du renseignement correspondent à deux de ces missions : celle de **recherche** et celle de **protection.**

I ESPIONNAGE

Pour le code pénal français, dans son article 73, **l'espionnage** est un crime, **commis par un étranger**, contre les intérêts de la défense nationale. Cela implique une participation humaine directe qui soit le fait de quelqu'un qui n'est pas français.
En élargissant la notion, on peut considérer que l'espionnage est la recherche par un étranger d'informations pouvant servir à compromettre les intérêts fondamentaux du pays dans lequel il agit.
Sous cette qualification, le Code pénal vise également certaines formes **d'actions**, comme l'aide à la pénétration de troupes étrangères ou les entreprises de démoralisation que je propose de laisser de côté car cela nous entraînerait trop loin. Nous en resterons donc à l'aspect recherche de l'espionnage.
Reprenons donc la mission de recherche. On peut distinguer deux types de recherches, celle de l'information ouverte et celle de l'information confidentielle. Pour cela, on a trois sources distinctes : les sources **ouvertes** proprement dites, les sources **techniques** et les sources **secrètes ou clandestines**.
Il va de soi que dans beaucoup d'esprits, le renseignement se limite aux sources clandestines, avec tout ce que cela peut comporter comme littérature. La réalité, comme vous le voyez, est toute autre et beaucoup plus complexe : l'espionnage n'est qu'un des aspects de la mission de recherche, si l'on se limite à un sens strict.
• Dans cette approche de l'espionnage, nous laisserons donc de côté les sources ouvertes, qui sont, selon un spécialiste américain, *"celles que personne n'a pensé à protéger ou à rendre secrètes"* [1] et dont l'exploitation n'est pas de l'espionnage.
On notera cependant que l'article 74 du Code pénal français condamne le rassemblement de renseignement *"dont la réunion et l'exploitation sont de nature à nuire à la défense nationale"*. Cela permettrait de considérer qu'il y aurait acte d'espionnage à rassembler dans le but de les communiquer à l'extérieur, des documentations d'accès totalement ouvert, comme des revues techniques, par exemple.
• Pour ce qui est des **sources techniques**, elles ne sont ni ouvertes, ni secrètes, dans le sens de caché.
Les sources techniques sont aujourd'hui très nombreuses et les anglo-saxons les classent en trois grands groupes : les transmissions, les images et l'acoustique.
Les **transmissions** SIGINT dans le vocabulaire technique du renseignement américain, peuvent être, à divers titres, des sources de renseignements.
On distingue, entre autres: le renseignement qui porte sur les communications (COMINT), c'est à dire les informations découlant de communications étrangères interceptées par d'autres que leurs destinataires légitimes; le renseignement électronique (ELINT) qui provient de l'émission de radiations électromagnétiques étrangères, autres que les communications, les explosions nucléaires ou autres sources de radio-activité; le renseignement télémétrique (TELINT) qui provient de l'interception de signaux étrangers destinés au guidage et au fonctionnement des satellites ou émanant de ceux-ci.
Compte tenu de leur nature, l'écoute des stations de radiodiffusion (*broadcast*) n'entre pas dans ce domaine mais ces émetteurs sont aussi suivis avec la plus grande attention par toutes les puissances. Il s'agit là en fait de recherche de renseignement ouvert. On peut ici donner quelques exemples : *La Voix nationale de l'Iran* , émise depuis Bakou, en U.R.S.S. se faisait passer pour l'expression de l'opposition au Shah d'Iran. La véhémence du ton de cette station, durant l'été 1978, contrastait avec la réserve officielle des médias soviétiques sur cette question à la même époque. L'écoute de cette station fut une interessante précision sur la stratégie poursuivie par les soviétiques et sur leur contribution à la "révolution islamique iranienne". Les émissions de radio sont écoutées de façon pratiquement systématique et l'on peut se procurer des documents écrits quotidiens rapportant ce qui y a été dit aux Etats-Unis, le FBIS ou surtout à la BBC, il existe un abonnement à SWB (Survey of World Broadcast) qui est modulé par continent.
Les **images** (PHOTINT) sont, évidemment, aussi des sources de renseignement. Il s'agit d'abord de l'interprétation de photographies provenant aussi bien de satellites que d'avions même si on est loin de la reconnaissance aérienne de la Première Guerre mondiale… Il s'agit également de procédés infra-rouges, de systèmes d'images par Radar et de tous les cas où des films ou des moyens électro-optiques sont utilisés pour enregistrer visuellement diverses formes d'énergie émises par des objets.
Le renseignement **acoustique** est une autre technique complexe de recherche de renseignement qui a connu un développement considérable ces dernières années, notamment dans le domaine de la collecte d'informations sous-marines.
Il existe, à côté de cela, d'autres sources qui n'entrent dans aucune de ces catégories, par exemple le renseignement **sismologique** destiné à détecter les expériences nucléaires (constatation,

localisation, intensité), et que l'on peut considérer comme relevant également du renseignement technique, ou le renseignement **informatique**, avec toutes les conséquences que l'on peut imaginer. Les moyens techniques sont en fait un véhicule de renseignement et tout dépend d'une part de la manière dont il est protégé, d'autre part, bien sur de son contenu. Mais, souvent les signes extérieurs du véhicule technique sont accessibles à peu près à tout le monde. Deux exemples : il y a des stations de radio qui émettent des chiffres à longueur de journée. Tout le monde peut les écouter; les comprendre est une autre histoire. Une photographie aérienne n'est une image mais tout dépend de ce que l'on photographie et d'où; mais si l'objet est photographiable, c'est qu'il est accessible à la vue, même s'il s'agit de celle d'un satellite.
L'intervention du facteur humain, qui rentre dans la définition de l'espionnage, dans la recherche d'informations à travers les sources techniques intervient à divers degrés, selon l'endroit, par exemple, où elle est pratiquée. On peut cependant distinguer l'exploitation des sources techniques de l'espionnage proprement dit qui n'est, je le répète, qu'un des aspects de la recherche du renseignement.
Le renseignement technique fournit cependant de grandes quantités de données de tout type qu'aucune source humaine (HUMINT) ne peut produire.
Cela a d'ailleurs pu conduire certains commentateurs à suggérer qu'il était possible de s'en contenter et d'éviter ainsi l'usage d'agents, avec les dangers et les compromissions que cela peut comporter. Cela fut surtout vrai aux Etats-Unis. Par exemple, l'ancien directeur adjoint du renseignement, l'Amiral Bobby R. Inman déclarait dans un interview en 1982 : *"Il y a eu une période où les **décideurs** croyaient que la photographie par satellite allait répondre à tous nos besoins"*. (2).
Ce point de vue semble aujourd'hui en voie d'abandon. Bobby Inman déclarait d'ailleurs dans le même document : *"Nous sommes tous un peu plus sages maintenant. Aucun analyste ne devrait être dépendant d'une source unique de renseignement. Les sources humaines comportent le risque de faire confiance à quelqu'un qui veut vous induire en erreur. Les sources techniques peuvent vous laisser sans accès à certains renseignements ou sans le contexte nécessaire à la compréhension de certains rapports"*. (3).

• A lui seul, aucun des aspects du renseignement technique, sources "ouvertes" comprises, n'est suffisant; tous se complètent, mais le renseignement humain, **en fait l'espionnage**, apporte souvent l'information clef nécessaire à une bonne compréhension du sujet.
D'ailleurs, au début des années 70, la direction du renseignement de la C.i.a. considérait qu'environ 30% des informations clef ou importantes utilisées pour ses études et rapports de synthèse provenaient de sources clandestines, humaines, donc de l'espionnage(4).

Donc, l'espionnage, c'est l'utilisation d'individus -on en revient à la définition du Code pénal- le recrutement d'agents et la manipulation de personnes. C'est la recherche d'informations qui sont, elles, hautement protégées par les Gouvernements et que l'on ne peut obtenir qu'à travers des moyens très spéciaux, voire détournés, et c'est un euphémisme.

Il faut savoir que l'espionnage est couteux, en termes de temps et d'énergies. Il nécessite du temps pour identifier et recruter les sources humaines qui pourraient avoir accès à l'information. Il y a exceptionnellement des préparations rapides. Le processus est généralement lent et laborieux et n'est généralement utilisé qu'en dernière extrémité.

Il y a des moyens d'améliorer les techniques classiques de l'espionnage, par exemple à travers la coopération avec les services de renseignement de pays amis : ils peuvent être d'excellentes sources d'information.

Il est aussi utile de rechercher les informations dont les réfugiés sont en possession, ou bien les émigrés, ou encore les défecteurs.

Moins évidente, mais néamoins d'importance potentielle dans un programme de collecte du renseignement, est l'aide que l'on peut attendre d'hommes d'affaires ayant des intérêts à l'étranger, et de ce fait confrontés à certains aspects techniques de la vie locale ou d'associations diverses. On peut discrètement leur demander de partager leurs connaissances avec leur Gouvernement.

L'espionnage c'est l'utilisation de l'homme, avec ses forces, mais aussi -dirais-je surtout ?- avec ses faiblesses pour essayer de savoir ce que les autres veulent cacher. Alors, parler de méthodes serait superflus, puisque dans ce type de stratégies indirectes, elles sont toutes envisageables et les plus étonnantes ont été rencontrées.

II CONTRE-ESPIONNAGE

Il s'agit des mesures de tout type destinées à protéger à la fois son territoire national compris dans le sens le plus large : installations, travaux de recherche, personnes, informations considérées comme "sensibles"… Protéger aussi son Gouvernement et ses diverses composantes d'opérations effectuées par des puissances étrangères. Protéger enfin ses outils de renseignement des tentatives de pénétration et de manipulation qui pourraient être faites par des services étrangers. Il peut aussi s'agir de manipulation d'agents étrangers ou d'opérations d'intoxication.
On emploie le plus souvent pour désigner la protection ainsi définie, les termes de **contre-espionnage** ou de **contre-ingérence**. On distingue l'ingérence de l'espionnage dont elle est un prolongement. Elle peut être définie comme le fait, pour un pays, de s'emparer de certains leviers de commande dans un autre pays. L'ingérence peut être politique, économique ou culturelle, le but étant toujours soit d'affaiblir, soit d'infléchir la politique du pays-cible.
L'*executive order* n° 12333 du 4 décembre 1981 donne la définition officielle du contre-espionnage aux Etats Unis : "*Le contre-espionnage regroupe les informations rassemblées et les activités conduites pour se protéger contre l'espionnage et les autres activités de renseignement, sabotage ou assassinats conduits pour ou au nom de puissances étrangères, organisations ou personnes, et les activités du terrorisme international…*" (5)

• Dans les activités de protection, on distingue traditionnellement des aspects passifs et actifs, **défensifs ou offensifs**, mais la ligne de séparation est floue et difficile à définir.
L'un consiste à **attendre passivement** les mouvements des agents des services adverses et à contrer des actes hostiles potentiels. En d'autres termes, cela comprend les mesures qui sont prises pour se protéger contre ce que l'adversaire pourrait être susceptible de faire.
Des mesures et activités caractéristiques du contre-espionnage passif consistent en programmes défensifs fondés sur des sources, en contre-mesures techniques de surveillance, en programmes d'information et d'éducation sur la sécurité, en appréciations de la vulnérabilité d'installations sensibles.
Le premier exemple consiste à identifier les principales cibles d'éventuelles menaces parmi les personnels et de mettre en place des programmes pour les contrôler. Cela implique la mise en place un système de "sources" à l'intérieur de l'administration ou l'entreprise menacée pour observer les actions des personnels susceptibles d'être vulnérables. Pour ce qui est du deuxième exemple, on peut se souvenir que ce sont ce type de contre-mesures qui ont mené à la découverte par les américains d'écoutes soviétiques sophistiquées dans leur salle "du grand Sceau" à leur ambassade de Moscou. Les autres exemples parlent d'eux-mêmes.
Ces activités passives, quoiqu'indispensables à une bonne sécurité intérieure, ne sont pas suffisantes. C'est pour cela que l'on utilise des **mesures actives** de contre-espionnage. (chasse au blaireau)
Elles consistent à entreprendre des actions offen
ngérence performant pour protéger ses droits civique, sa liberté et son indépendance il reste que, dans un système politique libéral, laisser un tel service dépasser des limites strictement définies entraîne le risque d'une remise en cause de ceux-ci.
Il faut donc trouver un point de compromis où il peut être nécessaire de tempérer **momentanément** l'exercice de ces droits et d'établir des méthodes légalement contrôlées de surveillance et de neutralisation des actions qui compromettraient nos intérêts nationaux. C'est par exemple l'objectif du *Foreign Intelligence Surveillance Act* (*FISA*) de 1978 qui est double: augmenter les capacités de renseignement des Etats-Unis tout en protégeant les droits constitutionnels des *"United States persons"* définies par le texte.
On peut donc avoir une vision plus large des activités de protection en constatant qu'elles ont, comme le renseignement pris dans son ensemble, trois facettes : l'acquisition des données, mais sur le théâtre des opérations internes, l'analyse de ces données(6),et l'action de protection proprement dite résultant des éléments précédents et comprenant également les activités de manipulation.
Ainsi conçu, le **contre-espionnage** apparait comme une discipline en lui-même. Se voyant fixer des objectifs à long terme, il doit aussi pouvoir saisir les opportunités immédiates, donc être en "prise directe" avec la direction politique au plus haut niveau.

Pour cela, les activités de **contre-espionnage**, comme celles de renseignement en général, doivent être protégées : si un Etat ne s'estime pas capable de garantir ses services spécialisés contre les indiscrétions ou des actions tendant à les affaiblir, je pense à certaines affaires de presse dans notre

pays, la logique veut qu'il supprime un instrument qu'il a rendu inutile. Mais de ce fait, il devient complètement ouvert et donc très vulnérable.(7)

Il est possible, pour conclure ce point, d'envisager une définition synthètique de ce que devrait être le contre-espionnage : un effort national de prévention contre l'infiltration des institutions et contre les activités d'espionnage, de subversion, par les services de renseignement et des groupes contrôlés par l'étranger.

Cette activité implique des missions d'enquête et de surveillance pour détecter la présence de services de renseignement étrangers, elle tente d'acquérir puis d'analyser des informations sur ces services et, dans certains cas, peut monter des opérations destinées à pénétrer, intoxiquer et manipuler à son avantage lesdits services ainsi que les organisations qui leurs sont inféodées. Ces activités s'effectuant sous le contrôle de l'Etat et, en France, sous la protection effective du Code pénal (secret de la défense nationale).

CONCLUSION

Il n'est pas facile de conclure sur un métier qui partage avec un autre le fait d'être le plus vieux du monde.

Cependant, il se dégage un certain nombre de lignes de force.

D'abord, l'espionnage et le contre espionnage ne sont pas des matières de roman.

C'est le théâtre le plus actif de la guerre permanente sans laquelle notre monde ne saurait vivre.

Cette guerre est une guerre totale : elle fait appel à toutes les forces vives des nations, militaires, au premier chef, mais aussi économiques, financières et concerne toutes les couches de population.

Son objectif est d'anéantir l'adversaire, tout au moins sur le plan idéologique en imposant insidieusement son hégémonie. Elle est totale parce qu'elle existe en dehors même des périodes de conflits armés tout en atteignant le même degré de cruauté. Elle est totale enfin parce qu'elle fait appel à toutes les stratégies indirectes dont l'espionnage et le contre-espionnage, avec les actions qu'ils impliquent sont des éléments clés.

Mais, l'espionnage et le contre-espionnage aujourd'hui sont aussi trop associés à la vie politique pour être des laissés pour compte. Ils sont l'un et l'autre des instruments de travail essentiels des décideurs qui leur permettent de prendre de faire des chois, de trancher en connaissance de cause pour arriver au meilleur résultat pour leur pays.

C'est dans cet esprit qu'il faut les préserver en évitant surtout de les galvauder.