



Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

« L'intelligence pour construire la stratégie et la décision de sécurité »

Toute décision a besoin d'être alimentée par l'information, on agit « en connaissance de cause » et pas uniquement par intuition. Cette recherche de la supériorité informationnelle pour décider concerne bien entendu le monde de l'entreprise¹, ce que caractérise le triptyque de l'intelligence économique au travers de la sécurité, de la veille et de la capacité d'influence. La conscience du caractère concurrentiel de l'information conditionne l'efficacité voire la survie d'une organisation non seulement pour des raisons liées à la communication mais aussi à l'action.

La sécurité publique est intéressée par ce besoin de supériorité informationnelle. Les forces de sécurité intérieure doivent faire face, elles aussi, à une concurrence, celles de leurs adversaires mais également celles de tiers voire de partenaires. Il s'agit bien de garantir les principes même de la **sécurité globale**² et ceux de la sécurité nationale³. En effet, il n'est plus concevable aujourd'hui de rester dans une posture réactive en attendant l'événement. L'anticipation conditionne la qualité de la décision, un niveau adapté d'engagement des ressources et une prédisposition pour des actions d'influence sur les décideurs. S'inscrire dans cette fonction connaissance-anticipation, ainsi qu'elle est précisée dans les livres blancs sur la défense⁴ et la sécurité⁵, s'impose aux forces de l'ordre aujourd'hui au travers de demandes que le monde politique formule⁶.

On est ici tenté d'aborder le renseignement. La pratique de la gestion de l'information invite à mieux préciser le domaine de l'information en matière de sécurité. Les praticiens évoquent le renseignement territorial, judiciaire, criminel, d'ordre public, opérationnel etc...au point de créer une zone de confusion dont certains peuvent jouer. La pratique comme la littérature permettent de nourrir la réflexion. Dans ce domaine, il faut reconnaître que les concepts sont anglo-saxons même si, sur les mots, la langue française apporte plus de sens.

Pour éviter de tomber dans une certaine aseptisation des termes, il convient de revenir sur ce qui constitue l'information au sens général et d'aborder dans le détail son contenu et son organisation. Ce cadre sémantique est essentiel pour aborder la construction de l'intelligence au travers d'un cycle qui a évolué dans sa pratique et fait face aujourd'hui à l'ère du numérique.

1 E. Delbecq et F. Debove, 2006, *Intelligence économique, questions judiciaires*, PUF p.29

2 INHESJ 2003 « Capacité d'assurer à une collectivité donnée et à ses membres, un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts d'où qu'ils viennent dans des conditions qui favorisent le développement sans rupture de la vie, des activités collectives et individuelles »

3 Art. L1111-1 du code de la défense.

4 Livre blanc sur la Défense de 2008, P.133

5 Livre blanc sur la sécurité publique de 2011, P119

6 Rapport d'information parlementaire N°2311 du 23 octobre 2014, *sur la lutte contre l'insécurité sur tout le territoire*, proposition N°33

I – Un cadre sémantique structuré

Le sens des mots conditionne les processus de réflexion et sert in fine l'action. La gestion de l'information s'appuie sur **un continuum cognitif**⁷. Il est alors possible de distinguer l'intelligence du renseignement.

Le continuum cognitif peut s'illustrer par une pyramide.

Sa base est constituée par les données. Les données sont brutes et nécessitent un traitement par des machines ou des hommes, sans quoi, elles présentent peu d'intérêts. Filtrées, recoupées, comparées et structurées, ces données deviennent élaborées.

Le niveau supérieur aux données est celui de l'information. Elle résulte de l'interprétation de données brutes et élaborées. Elle leur confère une signification et une valeur. L'information est également un fait ou un événement. A l'instar des données, l'information peut être protégée mais peut être également facilement accessible.

La troisième strate est identifiée par la connaissance, qui est une consolidation de l'information. La connaissance est propre à un individu, à une organisation ou à un domaine. L'accumulation d'informations permet d'améliorer la connaissance globale. Ainsi peut-on avoir des connaissances sur les trafics de stupéfiants et leur organisation. On peut donner ainsi une interprétation particulière à l'information. Cela peut s'illustrer également par la connaissance d'un territoire ou d'un secteur économique. L'accès à différentes études, rapports d'experts, à la littérature grise constitue une source majeure de connaissances.

Le quatrième niveau et sommet de la pyramide est l'intelligence. C'est le stade qui permet à un décideur ou à une structure de décision d'apprécier, de juger afin d'être en capacité de décider et de distinguer les éléments d'une situation. On revient ici à l'étymologie latine du mot intelligence, qui est la faculté de comprendre, de discerner dans ce qui a été cueilli, ramassé ou récupéré⁸. Derrière cette action, il y a bien entendu la notion de choix, de jugement et de sélection. L'intelligence a pour vocation de nourrir une réflexion stratégique ou d'alimenter le processus décisionnel. A l'instar du renseignement, l'intelligence doit produire une action. Elle se distingue de la compréhension qui reste une notion statique.

Cette définition de l'intelligence est l'occasion de faire le lien avec **le renseignement**. Ce dernier est en interaction avec les trois premiers niveaux du continuum. Le renseignement est une donnée ou une information remarquable, particulière telle que le précisent Jean-François Gayraud et François Farcy⁹. Il s'agit aussi du produit d'un cycle, qui s'est construit et a pris une valeur immédiatement utilisable. Le renseignement revêt un caractère confidentiel, voire secret, ce qui en fait un atout majeur dans la supériorité informationnelle. La compréhension s'enrichit du renseignement, devient intelligence et conduit à une décision à caractère opérationnel ou à des capacités d'influence fortes. Il existe un lien puissant entre ces deux termes.

S'agissant de prise de décision en matière de défense et de sécurité le renseignement revêt un caractère particulier. On peut noter qu'il n'est pas défini dans le domaine judiciaire. Sa sensibilité est réelle, elle fait écho aux moyens techniques et humains déployés pour l'obtenir. Pour les forces de police, le renseignement n'a de force qu'à la condition d'être transformé en acte judiciaire¹⁰. Dans tous les cas, l'État encadre cette recherche ainsi que son exploitation. Il s'agit même pour le plus sensible de le coordonner et de le contrôler. Enfin, les opérations initiées sur un renseignement présentent l'intérêt majeur d'alimenter le retour d'expérience et d'enrichir la connaissance d'un domaine ou d'un territoire, en l'intégrant éventuellement dans une réflexion plus globale, voire stratégique. Il n'y a pas de renseignement efficace sans intelligence.

7 Jerry Ratcliffe, 2009, *Intelligence led policing*, édition Willan Publishing, p.96 et CDEF, 2012, *rapport d'étude relatif aux principes de gestion de l'information opérationnelle dans les PC*, EMP50.201 p.21

8 Du latin *intelligentia*, dérivé de *intellegere*, composé du préfixe *inter* « entre » et du verbe *legere* « choisir, cueillir », qui signifie « comprendre », « discerner », « saisir par la pensée », « concevoir ».

9 Jean-François Gayraud et François Farcy, 2011, *Le renseignement criminel*, aux éditions CNRS, chapitre 1

10 C. Rault, 2010, *the French approach to counterterrorism*, <https://ctc.usma.edu/posts/the-french-approach-to-counterterrorism>.

La pratique montre que **l'intelligence est le socle de toute stratégie**, elle conditionne et consolide le renseignement dans la phase de décision opérationnelle. L'exemple britannique est ici manifeste. Dans le National Intelligence Model (NIM) de 2005¹¹, cette intelligence nourrit la réflexion stratégique, la réflexion tactique, l'étude territoriale d'une unité et le travail sur des cibles identifiées. L'éventail du terme anglais « intelligence » est donc très large. Sa traduction en français avec le terme « renseignement » prend une dimension tout aussi large et épouse parfaitement le quatrième niveau du continuum cognitif (voir supra). Ainsi, la Publication InterArmées 02-100 du 15 septembre 2009 (p.7) sur le concept interarmées du renseignement d'intérêt militaire définit le renseignement comme *portant sur la connaissance du monde et des phénomènes qui l'animent*. Le renseignement a donc une dimension opérationnelle dont la valeur est démultipliée quand il est considéré dans une approche globale, celle de l'intelligence.

II – La construction de l'intelligence

Elle s'inscrit dans un cycle et fait face aux enjeux de l'ère du numérique. Il en résulte l'émergence de nouvelles compétences.

C'est lors de la seconde guerre mondiale que **le cycle** prend naissance aux États-Unis. Les éléments du cycle sont plus ou moins identifiés au point qu'ils apparaissent dans un manuel de renseignement de l'armée américaine de 1940. Ce sont les lieutenants-colonels Robert Glass et Philip Davidson de l'école d'état-major qui les agencent dans un cycle¹². Kent Sherman reprend ce modèle dès 1949¹³. Il est constitué de quatre à six phases en fonction des États ou organisations. Le cycle est décrit comme **itératif**. Pour autant, la pratique remet en cause la linéarité de ce cycle. En effet, la phase exploitation peut inviter l'animateur de ce cycle à revenir sur la phase recherche voire sur la phase orientation. **Il est alors question d'interactivité**¹⁴ au sein même du cycle. Une phase sollicite la précédente d'initiative et par besoin. De plus, en abordant un territoire par les risques et menaces, le cycle permet de **combler l'absence de connaissance**¹⁵ et de rentrer dans une démarche proactive. Il peut s'agir même de développer **une phase observation avant d'initier la phase orientation** afin de déterminer les besoins. Cette évolution du cycle redonne de l'initiative aux échelons locaux. L'interactivité et le travail sur les risques permettent de **créer des liens** entre les différentes entités d'une même réflexion. De ces connexions naît la connaissance d'un thème étudié. C'est bien ici que se trouve la valeur ajoutée. Par ailleurs, il est important de souligner **l'émergence du « besoin de partager »**. Sans être en contradiction avec le « besoin d'en connaître », il contribue à la transparence de la construction de l'intelligence et conditionne le degré de confiance qu'on lui accorde.

Enfin, particulièrement en lien avec le renseignement, la notion d'immédiateté impose la prise de décision sur les éléments les plus actualisés. **La concurrence dans le domaine de l'information** est plus vive qu'elle ne l'a jamais été. Elle s'explique par la rapidité de la diffusion, par le rôle des médias et par la volonté de chaque partie prenante d'être en capacité de décider ou de participer à la décision. **La contraction du processus décisionnel** peut conduire à une concomitance entre la mise à disposition du produit du cycle et la décision. Cette situation représente un risque réel sur la qualité de la décision. Seul le socle de l'intelligence peut atténuer cette situation périlleuse pour une organisation. Le cycle vit, évolue et s'adapte, gagnant en souplesse, vitesse et modernité.

Le cadre juridique de l'exploitation des données à caractère personnel¹⁶ n'est pas une contrainte mais un impératif bénéfique. Il participe à un équilibre juridique, au respect des

11 NIM, 2005, Association of Chief Police Officers and National Centre Policing Excellence, p.64, §8.2.

12 R. Glass et P. Davidson, 1948, *Intelligence is for commanders*, P.5.

13 K. Sherman, 1949, *Strategic intelligence for American world policy*,

14 Peter Gill and Mark Pythian, 2012, *Understanding the intelligence cycle*, p.27, Studies in intelligence.

15 A.S. Hulnick, 2006, *What's wrong with the intelligence cycle*, international journal of intelligence Vol 21, p.960.

16 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

libertés fondamentales¹⁷ et à la transparence de l'action des services de l'État. De ce cadre résulte une qualité, celle de **la confiance**. L'intelligence, par son approche globale, ne fait pas appel aux données à caractère personnel. C'est ce qui la distingue du renseignement qui souffre en France, principalement de ce fait, d'une perception sociale négative. Il n'en demeure pas moins que ces données sont indispensables, et peuvent représenter des signaux d'alerte dans les cycles de l'intelligence et du renseignement.

Avec les données, c'est le *big-data* qui se profile. Enjeu actuel et à venir des données auxquelles il donne du sens, il met l'opérateur et l'analyste en capacité d'accéder, d'extraire, de trier et d'organiser une masse formidable d'éléments très diversifiés dans un temps toujours plus contraint. Même s'il n'en est qu'à ses débuts¹⁸, le *big-data* devient incontournable. Il permet de développer **l'analyse prédictive**. Internet ou plus précisément le **cyber-espace est une porte ouverte** sur un ensemble de données immédiatement accessibles. La source ouverte donne accès aux données à l'information, la connaissance y est également disponible. **La source ouverte n'exige pas de technique particulière et son coût est quasiment nul.** C'est donc une source précieuse. Le *big-data* et la source ouverte sont des ingrédients indispensables à ce cycle renouvelé pour aboutir à l'intelligence. Il ne s'agit plus de se contenter du renseignement de haut niveau. Le concept « *think global, act local* » prend ici toute sa force. Pour autant, cette culture d'accès à tout ce qu'il est possible de collecter peut cacher l'absence d'orientation. Ce serait tomber à nouveau dans une culture de performance sans autre ambition que celle du chiffre. **La surabondance de données et d'informations crée du « bruit »** qui ne permet plus de distinguer les signaux d'alerte d'un risque.

Un cycle renouvelé, un cadre juridique dédié et une profusion de sources nécessitent des compétences adaptées. C'est d'abord la **capacité technique**, indispensable pour exploiter l'outil informatique. Les applications métiers sont performantes et donnent accès à des données particulièrement précieuses. Il convient ensuite d'**organiser une veille** sur les différents réseaux et développer des savoir faire d'animation de capteurs. Une **capacité intellectuelle** est nécessaire pour sélectionner et associer les données, l'information et la connaissance. Manager l'information, au sens général du terme, est la fonction transversale du cycle de l'intelligence. L'analyste est désormais bien plus qu'un opérateur qui superpose des événements dans une synthèse. Il produit une valeur ajoutée, il **construit un raisonnement** en dégagant des hypothèses d'évolution. La **créativité** et l'imagination sont à encourager. Il s'agit de produire et non de reproduire. Cet analyste alimente ainsi la réflexion d'un décideur qui peut utiliser une réflexion poussée et argumentée pour une **prise de décision rapide**. Les qualités intuitives du décideur sont développées et non freinées. Ces compétences méritent d'être valorisées en s'appuyant sur un haut degré d'éducation qui révèle une maîtrise des outils de recherche, des **capacités d'analyse** et une **faculté d'adaptation**. Mais plus que des compétences et des métiers, c'est le développement d'une **culture de l'intelligence** qui s'impose.

Dans la décision qu'elle soit opérationnelle ou stratégique, la quête du Renseignement fait désormais place au paradigme de l'intelligence dans le fonctionnement du cycle. Pour une force de sécurité, **cette intelligence est territoriale**¹⁹ car elle permet de s'inscrire dans des politiques publiques nationales et locales pour produire en partenariat avec d'autres acteurs les actions qui vont prévenir les troubles, préparer les événements et accompagner les crises. D'aucuns parleront de **résilience**, il s'agit surtout de **comprendre rapidement les enjeux afin de prendre les bonnes décisions** dans des échelles temporelles toujours plus contraintes. Une force de sécurité doit s'appuyer sur les **nouvelles compétences** et développer une culture de l'intelligence. Les nouvelles technologies sont certes prometteuses, elles doivent cependant rester maîtrisées pour faciliter une action efficace.

17 Article 8 de la convention européenne des droits de l'Homme et des libertés fondamentales.

18 Steve Lohr, 15 décembre 2014, *Big hopes for big data hit reality*, International New York Times.

19 Didier Raciné, septembre 2013, *intelligence et territoire*, Revue de la Gendarmerie Nationale N°247.